

# Tivoli SecureWay Policy Director Base

## *Administratorhandbuch*

*Version 3.8*




# Tivoli SecureWay Policy Director Base

## *Administratorhandbuch*

*Version 3.8*

## Tivoli SecureWay Policy Director Base Administratorhandbuch

### Copyrightvermerk



### Marken








### Bemerkungen

Hinweise auf Produkte, Programme und Dienstleistungen von Tivoli Systems oder IBM in dieser Veröffentlichung bedeuten nicht, dass Tivoli Systems oder IBM diese in allen Ländern, in denen Tivoli Systems oder IBM vertreten ist, anbietet. Hinweise auf diese Produkte, Programme oder Dienstleistungen bedeuten nicht, dass nur Programme, Produkte oder Dienstleistungen von Tivoli Systems oder IBM verwendet werden können. Anstelle der Produkte, Programme oder Dienstleistungen von Tivoli Systems oder IBM können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von Tivoli Systems oder der IBM verletzen. Die Verantwortung für den Betrieb der Produkte, Programme oder Dienstleistungen in Verbindung mit Fremdprodukten und Fremddienstleistungen liegt beim Kunden, soweit solche Verbindungen nicht ausdrücklich von Tivoli Systems oder IBM bestätigt sind. Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es Tivoli Systems- oder IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanfragen sind schriftlich an IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France, zu richten. Anfragen an obige Adresse müssen auf Englisch formuliert werden.

# Inhaltsverzeichnis

# Vorwort

Willkommen beim *Tivoli SecureWay Policy Director Base Administratorhandbuch*.

Policy Director ist eine vollständige Berechtigungslösung für Web-, Client/Server-, MQ- und vorhandene traditionelle Anwendungen eines Unternehmens. Mit Hilfe der Policy Director-Berechtigung ist ein Unternehmen in der Lage, den Benutzerzugriff auf geschützte Daten und Ressourcen sicher zu steuern. Sie setzen Policy Director in Verbindung mit internetbasierten Standardanwendungen ein, um gut verwaltete, netzbasierte Anwendungen mit hoher Sicherheit zu erstellen.

Dieses Administratorhandbuch enthält umfassende Prozedurinformationen sowie Referenzinformationen für die Verwaltung von Policy Director-Servern und -Ressourcen. Dieses Handbuch enthält außerdem wertvolle Hintergrund- und Konzeptinformationen für die breitgefächerte Funktionalität von Policy Director.

## Zielgruppe

Zu der Zielgruppe für dieses Handbuch gehören:

- Sicherheitsadministratoren
- Administratoren für Systeminstallation und -einsatz
- Netzsystemadministratoren
- IT-Architekten
- Anwendungsentwickler

## Inhalt dieses Handbuchs

- **Kapitel 1: Übersicht über Policy Director**

  Dieses Kapitel enthält eine Einführung in wichtige Konzepte und Funktionen von Policy Director, wie z. B.: Policy Director-Kerntechnologien und -Komponenten, das Berechtigungsservicemodell sowie die Implementierung einer Sicherheits-Policy.

- **Kapitel 2: Geschützten Objektbereich verwalten**

  Dieses Kapitel beschreibt, wie Policy Director eine virtuelle Darstellung von Ressourcen in einem geschützten Objektbereich verwendet. Zwei Arten von Objektbereichen werden unterstützt: Flachdatei und Datenbank.

- **Kapitel 3: ACL-Policies verwenden**

  Dieses Kapitel dient als vollständige Referenz für ACL-Policies (ACL = Access Control List, Zugriffssteuerungsliste).

- **Kapitel 4: Policies für geschützte Objekte verwenden**

  Dieses Kapitel dient als vollständige Referenz für Policies für geschützte Objekte (POP-Policies).

- **Kapitel 5: Verwaltungs-Tasks delegieren**

  Dieses Kapitel erläutert, wie Policy Director die delegierte Verwaltung des Objektbereichs und Gruppenverwaltung unterstützt.

- **Kapitel 6: Policy Director-Server verwalten**

  Dieses Kapitel dient als technische Referenz für die Verwaltung und Anpassung des Policy Director-Serverbetriebs.

- **Kapitel 7: LDAP-Registrierungsdatenbank verwenden**

  Dieses Kapitel enthält eine Einführung in das LDAP-Protokoll/-Verzeichnis und ausführliche Informationen zur LDAP-Überbrückungskonfiguration.

- **Kapitel 8: Serveraktivität protokollieren und prüfen**

  Dieses Kapitel enthält eine vollständige Referenz für die Protokoll- und Prüffunktionen von Policy Director.

- **Anhang A: Referenz für Befehl pdadmin**
- **Anhang B: Referenz für ivmgrd.conf**
- **Anhang C: Referenz für ivacld.conf**
- **Anhang D: Referenz für ldap.conf**
- **Anhang E: Referenz für pd.conf**

## Schriftbildkonventionen

Dieses Handbuch verwendet mehrere Schriftbildkonventionen für spezielle Begriffe und Aktionen. Diese Konventionen haben folgende Bedeutung:

**Fett**
Befehlsnamen und Optionen, Schlüsselwörter und andere Informationen, die wörtlich verwendet werden müssen, werden **fett** angezeigt.

*Kursiv*
Variablen, Befehlsargumente und Werte, die Sie angeben müssen, werden *kursiv* angezeigt. Titel von Veröffentlichungen und spezielle Wörter oder Phrasen, die hervorgehoben werden, erscheinen ebenfalls *kursiv*.

`Monospace-Schrift`
Codebeispiele, Befehlszeilen, Bildschirmausgaben und Systemnachrichten werden in `Monospace-Schrift` angezeigt.

## Zugehörige Policy Director-Dokumente

In der folgenden Tabelle sind einige der verfügbaren Policy Director-Veröffentlichungen aufgeführt, die sich auf der Support Site von Tivoli SecureWay Policy Director befinden:

| Tivoli SecureWay Policy Director - Technische Dokumente |
|---|
| **Installationshandbücher** |
| Tivoli SecureWay Policy Director Base Installation Guide |
| Tivoli SecureWay Policy Director WebSEAL Installationshandbuch |
| **Administratorhandbücher** |
| Tivoli SecureWay Policy Director Base Administratorhandbuch (*dieses Dokument*) |
| Tivoli SecureWay Policy Director WebSEAL Administratorhandbuch |
| Tivoli SecureWay Policy Director Plug-in for Edge Server Administratorhandbuch |
| Tivoli SecureWay Policy Director Web Portal Manager Administratorhandbuch |

| Tivoli SecureWay Policy Director - Technische Dokumente |
|---|
| **Referenzdokumentation für Anwendungsentwickler** |
| Tivoli SecureWay Policy Director Authorization ADK Developer Reference |
| Tivoli SecureWay Policy Director Authorization API Java Wrappers Developer Reference |
| Tivoli SecureWay Policy Director Administration API Developer Reference |
| Tivoli SecureWay Policy Director WebSEAL Developer Reference |
| **Ergänzende Dokumentation** |
| Tivoli SecureWay Policy Director Release Notes |
| Tivoli SecureWay Policy Director Performance Tuning Guide |
| Tivoli SecureWay Policy Director Capacity Planning Guide |

## Auf Onlinedokumentation zugreifen

Die Website für die Tivoli-Kundenunterstützung (http://www.tivoli.com/support/) stellt Links zu den folgenden Dokumenten zur Verfügung:

- Technische Informationen, einschließlich Releasebeschreibungen, Installations- und Konfigurationshandbücher, Administratorhandbücher und Referenzdokumentationen für Anwendungsentwickler.
- Häufig gestellte Fragen (Frequently Asked Questions = FAQs)
- Informationen zum Herunterladen von Software

Das Customer Support Handbook (ein Handbuch zur Unterstützung von Services) finden Sie unter:

**http://www.tivoli.com/support/getting/.**

Sie können auf den Index der Tivoli-Onlineveröffentlichungen unter Verwendung der folgenden Adresse zugreifen: **http://www.tivoli.com/support/documents/**. Klicken Sie auf **Master Index**, um nach produktspezifischen Unterstützungsseiten zu suchen.

Technische Policy Director-Dokumentation nach Produktversion kann mit Hilfe folgender Adresse aufgerufen werden: **https://www.tivoli.com/secure/support/Prodman/html/AB.html#Security**.

Für einige Produkte ist die Dokumentation im PDF- und HTML-Format verfügbar. Übersetzte Dokumente stehen für einige Produkte ebenfalls zur Verfügung.

Für den Zugriff auf die meisten Dokumentationen benötigen Sie eine ID und ein Kennwort. Rufen Sie **http://www.tivoli.com/support/getting/** auf, um eine ID zur Verwendung auf der Unterstützungs-Website zu erhalten.

Wiederverkäufer sollten unter **http://www.tivoli.com/support/smb/index.html** die zusätzlichen Informationen bezüglich des Anforderns technischer Tivoli-Dokumentation und Unterstützung lesen.

Geschäftspartner sollten den Abschnitt „Dokumentation bestellen" auf Seite xvii im Vorwort lesen. Dieser Abschnitt enthält weitere Informationen über das Bestellen von technischer Tivoli-Dokumentation.

## Dokumentation bestellen

Tivoli-Dokumentation kann online unter

**http://www.tivoli.com/support/Prodman/html/pub_order.html** bestellt werden.

## Rückmeldung über Produktdokumentation

Wir sind sehr daran interessiert, Ihre Meinung über Tivoli-Produkte und -Dokumentation zu hören, und wir freuen uns über Verbesserungsvorschläge. Wenn Sie Kommentare oder Vorschläge haben, die unsere Produkte und Dokumentation betreffen, können Sie uns auf folgende Weise benachrichtigen:

- Senden Sie eine E-Mail an **pubs@tivoli.com**.
- Füllen Sie das Formular für die Kundenrückmeldung unter **http://www.tivoli.com/support/survey/** aus.

## Kundenunterstützung benachrichtigen

Das *Tivoli Customer Support Handbook* auf folgender Website:

**http://www.tivoli.com/support/handbook/**

enthält Informationen zu allen Aspekten der Tivoli-Kundenunterstützung. Hierzu gehören:

- Registrierung und Auswählbarkeit
- Angaben zum Anfordern von Unterstützung, abhängig von der Wertigkeit des Problems
- Telefonnummern und E-Mail-Adressen, abhängig von dem jeweiligen Land
- Informationen, die gesammelt werden müssen, bevor Unterstützung angefordert wird



# Übersicht über Policy Director

Policy Director ist eine vollständige Berechtigungslösung für Web-, Client/Server-, PDOS- (Policy Director for Operating Systems), PDMQ- (Policy Director for MQ Series) und traditionelle (vorhandene) Anwendungen eines Unternehmens. Mit Hilfe der Policy Director-Berechtigung ist ein Unternehmen in der Lage, den Benutzerzugriff auf geschützte Daten und Ressourcen sicher zu steuern.

Durch die Bereitstellung einer zentralen, flexiblen und skalierbaren Zugriffssteuerung ermöglicht Policy Director den Aufbau einer im höchsten Maß sicheren und optimal verwalteten netzbasierten Anwendungs- und e-business-Infrastruktur.

Stichwortindex:

## Unternehmensnetz sichern

In vielen Unternehmen werden das öffentliche Internet und private Intranets inzwischen als effektive und unverzichtbare Medien für die globale Kommunikation eingesetzt. E-Commerce, oder e-business, ist in kurzer Zeit zu einer wesentlichen Komponente vieler Marketingstrategien geworden. Ausbildungseinrichtungen nutzen das Internet für den Fernunterricht. Mit Hilfe der Onlinedienste können Einzelpersonen E-Mails senden und die nahezu unerschöpfliche Ressourcenquelle des World Wide Web nutzen. Traditionelle Anwendungen, wie z. B. TELNET und POP3, sind weiterhin als wichtige Netzservices vorhanden.

In den Unternehmen setzt sich die Erkenntnis durch, dass mit Hilfe der Internet-Methoden Lieferkettenverbindungen verbessert, die Zusammenarbeit mit Geschäftspartnern erleichtert und die Kundenverbindungen verstärkt werden können. Voraussetzung hierfür ist jedoch, dass Unternehmensressourcen mit einem hohen Maß an Sicherheit exponiert werden können. Unternehmen sind bereit, das Internet als globales Handels- und Vertriebsmedium einzusetzen, wurden bisher jedoch durch den Mangel an erprobten Sicherheitsstrategien und Verwaltungssystemen daran gehindert.

Policy Director ist eine Verwaltungslösung für die Informationspolitik, die Unternehmen zentrale Netzsicherheitsservices zur Verfügung stellt, mit denen die Sicherheitsstrategie eines Unternehmens konsequent implementiert und verwaltet werden kann.

Policy Director stellt die drei Hauptanforderungen für ausgeglichene Sicherheitslösungen zur Verfügung:

- Eine Reihe von Lösungen für den Aufbau einer Netzumgebung mit hoher Sicherheit
- Praktische und intuitive Verwaltungs-Tools für eine sichere zentrale Verwaltung
- Sicherheitsmechanismen, die berechtigte Client-Aktivitäten auf dem Netz nicht behindern

## Methoden und Definitionen der Netzsicherheit

Folgende Netzsicherheitsservices und -begriffe sind für die Beschreibung von Policy Director in diesem Dokument von Bedeutung:

- **Gesicherte Domäne** — Eine Gruppe von Benutzern, Systemen und Ressourcen, die allgemeine Services gemeinsam benutzen und in der Regel einem gemeinsamen Zweck dienen.
- **ACL-Policies (ACL = Access Control List, Zugriffssteuerungsliste)** — Der Sicherheitsmechanismus von Policy Director, der Benutzern und Gruppen die Berechtigungen für bestimmte Operationen (Aktionen) für geschützte Ressourcen zur Verfügung stellt.
- **Authentifizierung** — Die Identifikation jedes Benutzers, der sich an einer gesicherten Domäne anmelden will.
- **Berechtigungserteilung** — Die Feststellung (durch den Berechtigungsservice), ob ein Benutzer über die Berechtigung verfügt, eine Operation für eine geschützte Ressource auszuführen.
- **Berechtigung** — Während der Authentifizierung zugeordnete detaillierte Informationen, die den Benutzer, die Gruppenbeziehungen (falls vorhanden) und andere sicherheitsrelevante Identitätsattribute beschreiben.
- **Verschlüsselung** — Die Umwandlung von elektronischen Daten in einen Geheimcode, der die Daten vor unberechtigtem Einblick schützt. Die Verschlüsselung vereinfacht die als **Zugriffscode** bezeichnete Sicherheitsbedingung.
- **Integrität** — Die Bedingung, dass elektronische Daten zwischen Sende- und Empfangszeit unverändert bleiben.
- **POP-Policy** (POP = Protected Object Policy, Policy für geschütztes Objekt) — Der Sicherheitsmechanismus von Policy Director, der spezielle Bedingungen für den Zugriff auf eine geschützte Ressource nach einer erfolgreichen ACL-Policy-Prüfung vorschreibt.

- **Geschützter Objektbereich** — Die virtuelle Objektdarstellung tatsächlicher Systemressourcen, die zum Anwenden von ACL- und POP-Policies und vom Berechtigungsservice verwendet wird.
- **Registrierungsdatenbank** — Der Datenspeicher (z. B. LDAP), in dem die Benutzerinformationen für Benutzer und Gruppen, die eine Berechtigung für die gesicherte Domäne besitzen, verwaltet werden.
- **Skalierbarkeit** — Die Fähigkeit eines Netzsystems, eine zunehmende Anzahl an Benutzern, die auf Ressourcen zugreifen, zu bearbeiten.
- **Sicherungsstufe** — Der Grad der Datensicherheit, der sich aus einer Kombination aus Authentifizierungs-, Integritäts- und Zugriffscodebedingungen zusammensetzt.

## Netzsicherheit — Allgemeine Hinweise

Sowohl das weltweite öffentliche Internet als auch firmeninterne Intranets sind mit heterogenen Datenverarbeitungssystemen, Anwendungen und Netzen verbunden. Diese Mischung unterschiedlicher Hardware und Software wirkt sich normalerweise wie folgt auf ein Netz aus:

- Keine zentrale Kontrolle der Sicherheit für Anwendungen
- Keine einheitliche URL-Namenskonvention (URL = Uniform Resource Locator)
- Keine allgemeine Unterstützung für Hochverfügbarkeitsanwendungen
- Keine allgemeine Unterstützung für skalierbaren Zuwachs

Neue Geschäftsmodelle machen es erforderlich, dass Unternehmen Ihre Informationsquellen in einem bisher undenkbaren Maß exponieren. Diese Unternehmen müssen sich darauf verlassen können, dass sie den Zugriff auf diese Quellen sicher kontrollieren können.

Die Verwaltung von Policies und Benutzern in verteilten Netzen hat sich als schwere Aufgabe für IT-Manager (IT = Information Technology) erwiesen, insbesondere seit einzelne Anwendungs- und Systemlieferanten eigene Berechtigungen implementieren.

In den Unternehmen erkennt man, dass die Entwicklung neuer Berechtigungsservices für jede Unternehmensanwendung ein kostspieliger Prozess ist, der in einer schwer zu verwaltenden Infrastruktur resultiert. Ein zentraler Berechtigungsservice, auf den Entwickler über eine standardisierte API zugreifen, könnte Zeitaufwand und Gesamtkosten beträchtlich reduzieren.

Ein zentrales Netzsicherheitsverwaltungssystem muss folgende Anforderungen erfüllen:

- Koexistenz mit vorhandenen Firewall- und Authentifizierungsarchitekturen und/oder Verbesserung dieser Architekturen
- Integration oder Koexistenz mit Netz- und Anwendungsverwaltungs-Frameworks
- Anwendungsunabhängigkeit

## Einführung in Policy Director

Policy Director ist eine vollständige Verwaltungslösung für Berechtigungs- und Netzsicherheits-Policies, die unübertroffenen Endpunkt-zu-Endpunkt-Schutz für Ressourcen in geographisch voneinander getrennten Intranets und Extranets zur Verfügung stellt.

Zusätzlich zur Verwaltungsfunktion für Sicherheits-Policies unterstützt Policy Director Authentifizierungs-, Berechtigungs-, Datensicherheits- und Ressourcenverwaltungsfunktionen. Sie setzen Policy Director in Verbindung mit internetbasierten Standardanwendungen ein, um gut verwaltete, netzbasierte Intranets mit hoher Sicherheit zu erstellen.

Die Kernkomponenten von Policy Director:

- Authentifizierungs-Framework

  Policy Director stellt eine Vielzahl von integrierten Authentifizierungsfunktionen zur Verfügung und unterstützt externe Authentifizierungsfunktionen.

- Berechtigungs-Framework

  Der Policy-Berechtigungsservice, auf den über eine Standardberechtigungs-API zugegriffen wird, stellt Berechtigungserteilungen und -ablehnungen für Zugriffsanforderungen für native Policy Director-Server und für Anwendungen anderer Hersteller zur Verfügung.

Mit Policy Director können Unternehmen jetzt den Zugriff auf private interne, netzbasierte Ressourcen sicher verwalten und die breite Konnektivität und Benutzerfreundlichkeit des öffentlichen Internets nutzen. Policy Director kann in Verbindung mit einem unternehmensinternen Firewall-System das Unternehmens-Intranet vor unbefugtem Zugriff und Eindringen vollständig schützen.

## Standard-API des Berechtigungsservice

Der Berechtigungsservice ist eine kritische Komponente der Sicherheitsarchitektur einer Anwendung. Nachdem ein Benutzer den Authentifizierungsprozess abgeschlossen hat, stellt der Berechtigungsservice fest, auf welche Services und Informationen der Benutzer zugreifen kann, um so die Unternehmenspolitik weiter umzusetzen.

Ein Benutzer, der auf ein webbasiertes Konto zugreift, könnte z. B. persönliche Kontodaten anzeigen, nachdem ein Server die Identität, Berechtigung und Berechtigungsattribute dieses Benutzer geprüft hat.

Die standardisierte Berechtigungs-API gestattet Anwendungen, Aufrufe an den zentralen Berechtigungsservice zu senden, wodurch es für Entwickler nicht mehr erforderlich ist, Berechtigungscode für jede neue Anwendung zu schreiben.

Mit Hilfe der Berechtigungs-API können Unternehmen für alle Anwendungen ein standardisiertes, gesichertes Berechtigungs-Framework verwenden. Mit der Berechtigungs-API sind Unternehmen in der Lage, den Zugriff auf Ressourcen in ihren Netzen besser zu steuern.

# Policy Director — Kerntechnologien

Die Netzsicherheitsverwaltung von Policy Director bietet und unterstützt folgende Kerntechnologien:

- Authentifizierung
- Berechtigungserteilung
- Sicherungsstufe
- Skalierbarkeit
- Nachprüfbarkeit
- Zentrale Verwaltung

## Authentifizierung

Die Authentifizierung ist der erste Schritt, den ein Client ausführen muss, wenn er eine Ressource in einem Netz anfordert, das durch Policy Director geschützt wird. Der Authentifizierungsprozess ist normalerweise von den spezifischen Anforderungen der Serviceanwendung abhängig. Policy Director gestattet eine höchst flexible Handhabung der Authentifizierung durch Verwendung der Berechtigungs-API.

Policy Director Base stellt integrierte Unterstützung der Authentifizierung von Benutzernamen und Kennwörtern durch die Berechtigungs-API zur Verfügung. Anwendungsentwickler können beliebige angepasste Authentifizierungsverfahren erstellen, die die Berechtigungs-API verwenden.

## Berechtigungserteilung

- Policy Director-Berechtigungsservice
- ACL- und POP-Policies für feinkörnige Zugriffssteuerung
- Standardisierte Berechtigungs-API
- Fähigkeit, externe Berechtigungsservices zu verwenden

## Sicherungsstufe (Daten)

Die Sicherungsstufe gibt den Grad des Schutzes an, mit dem Policy Director alle Informationen schützt, die zwischen Client und Server

übertragen werden. Die Sicherungsstufe wird aus einer Kombination aus Verschlüsselungsstandards und Algorithmen zur Feststellung von Änderungen festgelegt.

Mögliche Sicherungsstufen:

- Standard-TCP-Übertragung (kein Schutz)
- Datenintegrität – Schützt Nachrichten (Datenströme) vor einer Änderung während der Netzübertragung
- Datenschutz – schützt Nachrichten vor einer Änderung oder Prüfung während der Netzübertragung

## Unterstützte Verschlüsselungsstandards

Policy Director unterstützt folgende Verschlüsselungen über SSL:

- 40-Bit RC2
- 128-Bit RC2
- 40-Bit RC4
- 128-Bit RC4
- 40-Bit DES
- 56-Bit DES
- 168-Bit Triple DES

## Gesicherte Übertragung

Policy Director unterstützt die Datenintegrität und den Datenschutz des SSL-Übertragungsprotokolls (SSL = Secure Socket Layer).

Das SSL-Handshake-Protokoll wurde durch die Netscape Communications Corporation entwickelt und stellt Datensicherheit und -schutz im Internet zur Verfügung. SSL verwendet öffentliche Schlüssel für die Authentifizierung und geheime Schlüssel für die Verschlüsselung von Daten, die über die SSL-Verbindung übertragen werden.

Policy Director unterstützt die SSL-Versionen 2 und 3.

## Skalierbarkeit

Die Skalierbarkeit ist die Fähigkeit, eine zunehmende Anzahl an Benutzern, die auf Ressourcen in der gesicherten Domäne zugreifen, zu bearbeiten. Policy Director stellt die Skalierbarkeit mit folgenden Methoden zur Verfügung:

- Servicereplikation
  - Authentifizierungsservices
  - Berechtigungsservices
  - Sicherheits-Policies
  - Datenverschlüsselungsservices
  - Prüfungsservices
- Front-End-Replikationsserver (WebSEAL)
  - Gespiegelte Ressourcen für hohe Verfügbarkeit
  - Lastausgleich für Client-Anforderungen
- Back-End-Replikationsserver (WebSEAL)
  - Back-End-Server können WebSEAL-Server oder Anwendungsserver eines anderen Herstellers sein
  - Gespiegelte Ressourcen (gemeinsamer Objektbereich) für hohe Verfügbarkeit
  - Zusätzlicher Inhalt und Ressourcen
  - Lastausgleich eingehender Anforderungen durch Junctions
- Optimierte Leistung durch Auslagern von Authentifizierungs- und Berechtigungsservices auf separate Server
- Skalierter Einsatz von Services ohne Zunahme des Verwaltungsaufwands

## Nachprüfbarkeit

Policy Director stellt eine Reihe von Protokoll- und Prüffunktionen zur Verfügung. Es gibt Protokolldateien, in denen alle Fehlernachrichten und Warnungen, die Policy Director-Server generieren, erfasst werden. Außerdem wird die Aktivität der Policy Director-Server in Prüfprotokolldateien überwacht.

### Protokolldateien:

- Policy Director-Serverprotokolldateien
- Servicenachrichten
- Standard-HTTP-Protokolldateien

### Prüfprotokolldateien:

- Policy Director-Serverprüfprotokolldateien

## Zentrale Verwaltung

- Web Portal Manager
- Befehlszeilendienstprogramm **pdadmin**

# Policy Director-Komponenten

Policy Director verfügt über Software für Client- und Serversysteme. Policy Director wird auf den Plattformen UNIX (einschließlich Solaris, AIX, HP-UX und Linux) und Windows NT/Windows 2000 unterstützt.

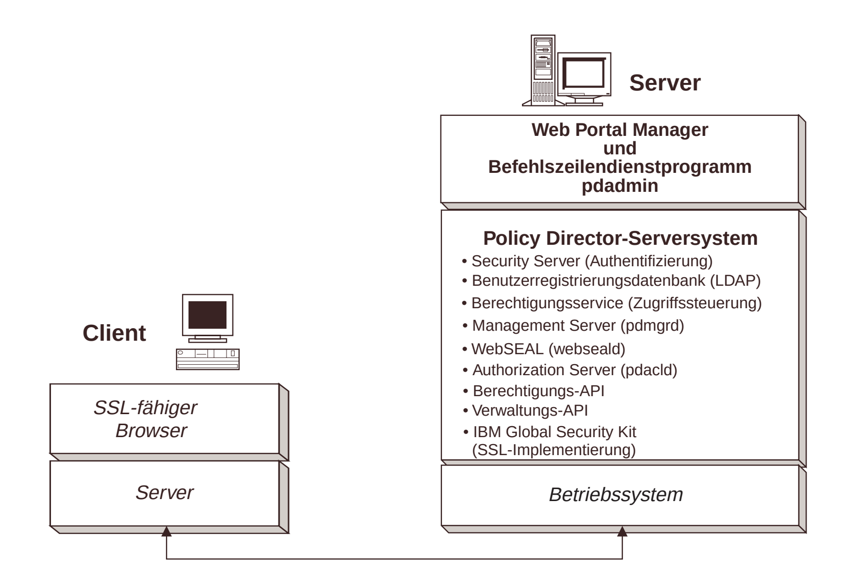



*Abbildung 1. Policy Director-Komponenten*

## Web Portal Manager

Web Portal Manager ist eine webbasierte Grafikanwendung, mit der die Sicherheits-Policy für die gesicherte Domäne von Policy Director verwaltet wird. Web Portal Manager stellt die Verwaltung von Benutzern, Gruppen, Berechtigungsklassen, Policies und der Bereitstellung des Anwendungszugriffs zur Verfügung.

Web Portal Manager verfügt außerdem über eine umfangreiche Gruppe von Stellvertreterverwaltungsservices, mit der die Benutzerverwaltung, Gruppen- und Berechtigungsklassenverwaltung, die Sicherheitsverwaltung sowie die Bereitstellung des Anwendungszugriffs für Teilnehmer (Subdomänen) im Geschäftssystem delegiert werden kann. Diese Subdomänen können die Verwaltung weiter an sichere Subdomänen unter ihrer Steuerung delegieren, wodurch mehrstufiges Delegieren und eine Verwaltungshierarchie auf der Grundlage von Berechtigungsklassen unterstützt wird.

## Befehlszeilendienstprogramm pdadmin

Das Befehlszeilendienstprogramm **pdadmin** bietet die Möglichkeit, alle Policy Director-Verwaltungs-Tasks auszuführen. Web Portal Manager stellt eine begrenzte Anzahl dieser Verwaltungs-Tasks zur Verfügung.

## Security Server

Der Security Server ist der LDAP-Server, der Authentifizierungsservices zur Verfügung stellt und eine zentrale Registrierungsdatenbank verwaltet, die Kontoeinträge für alle gültigen Benutzer der gesicherten Domäne enthält.

Der Security Server führt zwei wichtige Aufgaben aus:

- Definiert die Gruppen und Organisationen, zu denen der Benutzer gehört, sowie die Berechtigungsklassen, die der Benutzer übernehmen kann. Diese Informationen werden in einer zentralen Registrierungsdatenbank gespeichert. Der Berechtigungsservice berücksichtigt diese Informationen bei Berechtigungsentscheidungen.
- Stellt Authentifizierungsservices für alle Anmeldeversuche zur Verfügung.

Der Sicherheitsserver kann die Registrierungsdatenbank innerhalb der gesicherten Domäne replizieren (vervielfältigen), um einen Single Point of Failure (einzelner Fehlerpunkt) zu vermeiden. Der Sicherheitsserver ist für die Aktualisierung aller Replikationsdatenbanken verantwortlich, sobald eine Änderung in der Hauptregistrierungsdatenbank auftritt.

## Management Server

Der Management Server (**pdmgrd**) verwaltet die Hauptberechtigungs-Policy-Datenbank für die gesicherte Domäne. Er ist außerdem verantwortlich für die Aktualisierung aller Berechtigungsdatenbankreplikationen innerhalb der gesicherten Domäne. Der Management Server verwaltet außerdem die Positionsinformationen für die anderen Policy Director-Server in der gesicherten Domäne.

## WebSEAL

WebSEAL (**webseald**) ist ein Ressourcenschutzmanager, der feinkörnige HTTP- und HTTPS-Zugriffssteuerung zur Verfügung stellt.

WebSEAL ist ein Webserver mit hoher Leistung und mehreren Threads, der HTTP- und HTTPS-Anforderungen akzeptiert. WebSEAL verwaltet die Zugriffssteuerung für folgende Ressourcen: URL-Adressen, URL-basierte reguläre Ausdrücke, CGI-Programme, HTML-Dateien, Java-Servlets und Java-Klassendateien.

WebSEAL sichert und verwaltet als Junction-Server Webserver anderer Hersteller mit Hilfe der WebSEAL-Junction-Methode. WebSEAL-Junctions ermöglichen Ihnen, dem Webbereich zusätzliche Serverdateisysteme zuzuordnen und die Ressourcen als einzelnen Objektbereich anzuzeigen.

WebSEAL kann für die Bereitstellung von Einzelanmeldungsfunktionen für webbasierte Ressourcen verwendet werden. Der Benutzer kann sich über Standard-SSL bei WebSEAL authentifizieren. WebSEAL stellt dann den Benutzer dar, der HTTP-Basis- und Hash-Wert-Authentifizierung verwendet. WebSEAL kann die Benutzeridentität auch als CGI-Variable übergeben.

## Berechtigungs-API

Das Policy Director Application Development Kit (ADK) verfügt über eine Berechtigungs-API, mit deren Hilfe Entwickler Policy Director-Sicherheit und -Berechtigung direkt in Unternehmensanwendungen eingliedern können. Die Berechtigungs-API stellt direkten Zugriff auf die Berechtigungsservices zur Verfügung, was bedeutet, dass Anwendungsentwickler nicht mehr für jede Anwendung Berechtigungscode schreiben müssen.

Die Berechtigungs-API reduziert Anwendungsentwicklungszeit und -kosten. Da die gesamte Netzsicherheit zentral durch Policy Director verwaltet wird, werden Anschaffungs- und Betriebskosten und die Wahrscheinlichkeit von Sicherheitsübertretungen beträchtlich verringert.

Die der Berechtigungs-API zugrundeliegende Technologie wurde nach einstimmigem Urteil der Security Working Group von Open Group für die schnelle Normung angenommen.

### Verwaltungs-API

Die Verwaltungs-API stellt eine vollständige Funktionsgruppe für das Dienstprogramm **pdadmin** zur Verfügung. Mit Hilfe der Funktionen können Anwendungen eines anderen Herstellers Policy Director-Objekte (ACLs, Aktionen, Objekte, POPs, Server, Benutzer, Gruppen, Policies) programmatisch verwalten.

### Policy Director Authorization Server

Im Berechtigungsmodus für fernen Cache verwenden Anwendungen die Funktionsaufrufe, die die Berechtigungs-API zur Verfügung stellt, um mit dem Authorization Server (**pdacld**) zu kommunizieren. Der Authorization Server verwaltet eine Replikation (Kopie) der Berechtigungs-Policy-Datenbank und fungiert als Auswerter für die Berechtigungsentscheidungsfindung.

Die API leitet eine Berechtigungsentscheidungsanforderung an den Authorization Server weiter. Der Authorization Server liefert eine Empfehlung gemäß der Sicherheits-Policy. Der Server kann auch einen Protokolleintrag schreiben, der die Details der Berechtigungsanforderung enthält.

### IBM Global Security Kit (GSKit)

Policy Director verwendet die GSKit-Implementierung des SSL-Protokolls (GSKit = IBM Global Security Kit). Administratoren verwalten X.509-Zertifikate mit Hilfe des GSKit-Dienstprogramms **iKeyman**.

## Erläuterungen zur Berechtigung: Konzeptionelles Modell

Wenn Server die Sicherheit in einer gesicherten Domäne aktivieren, muss sich jeder Client identifizieren. Die Sicherheits-Policy legt wiederum fest, ob der betreffende Client eine Operation für eine angeforderte Ressource ausführen darf.

Da der Zugriff auf jede Ressource in einer gesicherten Domäne durch einen Server gesteuert wird, können die Authentifizierungs- und Berechtigungsanforderungen des Servers umfassende Netzsicherheit zur Verfügung stellen.

In Sicherheitssystemen wird zwischen Berechtigung und Authentifizierung unterschieden. Die Berechtigung legt fest, ob ein authentifizierter Client das Recht hat, eine Operation für eine bestimmte Ressource in einer gesicherten Domäne auszuführen. Die Authentifizierung stellt sicher, dass der Benutzer tatsächlich die angebliche Person ist. Sie sagt jedoch nichts über die Berechtigung für Operationen mit einer geschützten Ressource aus.

Im Policy Director-Berechtigungsmodell wird die Berechtigungs-Policy unabhängig von der Benutzerauthentifizierung implementiert. Benutzer können ihre Identität mit Hilfe von öffentlichen/privaten Schlüsseln, geheimen Schlüsseln oder mit Hilfe benutzerdefinierter Mechanismen prüfen lassen.

Teil des Authentifizierungsprozesses ist der Erwerb einer Berechtigung, die die Identität des Clients beschreibt. Durch einen Berechtigungsservice getroffene Berechtigungsentscheidungen beruhen auf Benutzerberechtigungen.

Die Ressourcen in einer gesicherten Domäne erhalten eine Sicherungsstufe, die durch die Sicherheits-Policy der Domäne vorgeschrieben ist. Die Sicherheits-Policy definiert die legitimen Mitglieder der gesicherten Domäne sowie die Schutzstufe, die jede Ressource, die Schutz benötigt, umgibt.

Der Berechtigungsprozess besteht aus folgenden Basiskomponenten:

- Ein **Ressourcenmanager**, der für die Implementierung der angeforderten Operation verantwortlich ist, wenn Berechtigung erteilt wird. Eine Komponente des Ressourcenmanagers ist eine **Komponente zur zwingenden Anwendung der definierten Policy**, die die Anforderung zur Verarbeitung an den Berechtigungsservice weiterleitet.

- Ein **Berechtigungsservice**, der die Entscheidungsfindung für die Anforderung ausführt.

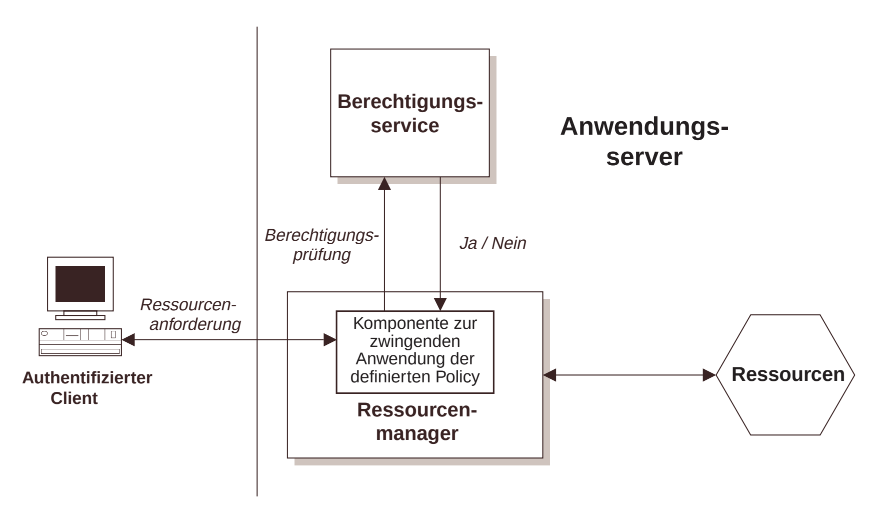



*Abbildung 2. Allgemeines Berechtigungsmodell*

In herkömmlichen Anwendungen sind die Komponente zur zwingenden Anwendung der definierten Policy und der Ressourcenmanager in einem Prozess zusammengefasst. Beispiele dieser Struktur sind Policy Director WebSEAL und Anwendungen anderer Hersteller.

Die unabhängige Funktionalität dieser Berechtigungskomponenten gestattet viel Flexibilität für den Entwurf der Sicherheitsstrategie.

Diese Unabhängigkeit gestattet Sicherheitsadministratoren beispielsweise die Steuerung folgender Punkte:

- Wo sich die Prozesse befinden
- Wer den Code für die Prozesse schreibt
- Wie die Prozesse ihre Tasks ausführen

## Vorteile eines Standardberechtigungsservice

Die Berechtigung ist in den meisten Systemen (traditionelle und neue) fest mit einzelnen Anwendungen verknüpft. Unternehmen erstellen normalerweise im Laufe der Zeit ihren Geschäftsanforderungen entsprechende Anwendungen. Viele dieser Anwendungen erfordern eine bestimmte Art der Berechtigung.

Daraus ergibt sich häufig eine Vielzahl von Anwendungen mit verschiedenen Berechtigungsimplementierungen. Diese Berechtigungsimplementierungen des Eigentümers erfordern separate Verwaltung, lassen sich schwer integrieren und verursachen höhere Kosten.

Ein verteilter Berechtigungsservice kann diesen unabhängigen Anwendungen eine Standardmethode für die Berechtigungsentscheidungsfindung zur Verfügung stellen. Vorteile eines derartigen Standardberechtigungsservice:

- Kostenminderung für Entwicklung und Verwaltung des Zugriffs auf Anwendungen
- Minderung der Anschaffungs- und Betriebskosten und der Verwaltungskosten separater Berechtigungssysteme
- Durchsetzung vorhandener Sicherheitsinfrastruktur
- Sicherere Eröffnung neuer Unternehmen
- Aktivierung neuerer und unterschiedlicherer Anwendungsarten
- Kürzere Entwicklungszyklen
- Sichere gemeinsame Informationsnutzung

## Einführung in den Policy Director-Berechtigungs-service

Policy Director wird in vorhandene, traditionelle und in sich entwickelnde Infrastrukturen integriert und stellt gesicherte, zentrale Policy-Verwaltungsfähigkeit zur Verfügung. Der Policy Director-Berechtigungsservice bietet in Verbindung mit Ressourcenmanagern (z. B. WebSEAL) eine Standardberechtigungsmethode für Unternehmensnetzsysteme.

Vorhandene Anwendungen können den Berechtigungsservice nutzen. Die Berechtigungs-Policy basiert auf Benutzer- oder Gruppenberechtigungsklassen und kann auf Netzserver, einzelne Transaktionen oder Datenbankanforderungen, spezifische webbasierte Informationen, Verwaltungsaktivitäten und benutzerdefinierte Objekte angewendet werden.

Die Berechtigungs-API (siehe „Policy Director-Berechtigungs-API" auf Seite 35) gestattet vorhandenen Anwendungen Aufrufe an den Berechtigungsservice durchzuführen, der wiederum Entscheidungen gemäß der Sicherheits-Policy des Unternehmens trifft.

Der Policy Director Berechtigungsservice ist außerdem erweiterbar und kann so konfiguriert werden, dass mit Hilfe der Plug-In-Schnittstelle des externen Berechtigungsservice andere Berechtigungsservices für zusätzliche Verarbeitung angefordert werden können.

## Vorteile des Policy Director-Berechtigungsservice

Der Berechtigungsservice bietet folgende Vorteile:

- Der Service ist anwendungsunabhängig
- Der Service verwendet eine sprachunabhängige Standardberechtigungscodierung (die Berechtigungs-API)
- Der Service ist zentral und einfach verwaltet. Wenn beispielsweise ein neuer Mitarbeiter hinzukommt, muss nur die Berechtigungsdatenbank in einer Zentrale und nicht in mehreren Systemen geändert werden.
- Der Service richtet sich an die Anwendung von Sicherheitsservices in einer heterogenen, plattformübergreifenden Umgebung
- Der Service integriert vorhandene andere Berechtigungssysteme durch eine externe Berechtigungsservicefähigkeit
- Der Service verfügt über eine skalierbare und flexible Architektur, die auf einfache Weise in eine vorhandene Infrastruktur integriert werden kann
- Der Service ermöglicht mehrschichtige Berechtigung — ein Berechtigungspaket kann durch die verschiedenen Schichten eines Anwendungsprozesses oder einer Transaktion geleitet werden
- Der Service verwendet ein allgemeines und effektives Prüfungsmodell
- Der Service ist unabhängig von Authentifizierungsmethoden

# Policy Director-Berechtigungsservice

Der Policy Director-Berechtigungsservice ist verantwortlich für die Berechtigungsentscheidungsfindung, die die Durchführung einer Netzsicherheits-Policy unterstützt. Durch den Berechtigungsservice getroffene Berechtigungsentscheidungen resultieren in der Genehmigung oder in der Ablehnung von Client-Anforderungen zur Durchführung von Operationen für geschützte Ressourcen in der gesicherten Domäne.

## Komponenten

Der Berechtigungsservice besteht aus drei Basiskomponenten:

- Hauptberechtigungs-Policy-Datenbank
- Verwaltungsserver
- Auswertungsprogramm für Berechtigungsentscheidungsfindung

### Hauptberechtigungs-Policy-Datenbank

Die Hauptberechtigungs-Policy-Datenbank enthält die Sicherheits-Policy-Informationen für alle Ressourcen in der gesicherten Domäne. Die Datenbank enthält außerdem alle erforderlichen Berechtigungsinformationen, die den Mitgliedern der gesicherten Domäne zugeordnet sind.

Den Inhalt dieser Datenbank erfassen und ändern Sie mit dem Web Portal Manager.

### Management Server (pdmgrd)

Der Management Server verwaltet die Hauptberechtigungs-Policy-Datenbank, repliziert diese Policy-Informationen innerhalb der gesicherten Domäne und aktualisiert die Datenbankreplikationen, sobald die Hauptdatenbank geändert wird. Der Management Server verwaltet außerdem die Positionsinformationen für die anderen Policy Director- und Nicht-Policy Director-Server in der gesicherten Domäne.

**Anmerkung:** Eine gesicherte Domäne darf nur ein Exemplar des Management Servers enthalten.

## Berechtigungsauswertungsprogramm

Das Berechtigungsauswertungsprogramm ist der Entscheidungsfindungsprozess, der die Fähigkeit eines Clients festlegt, gemäß der Sicherheits-Policy auf eine geschützte Ressource zuzugreifen. Das Auswertungsprogramm gibt seine Empfehlung an den Ressourcenmanager weiter, der entsprechend reagiert.

Für jedes Auswertungsprogramm können Replikationsparameter der Registrierungsdatenbank konfiguriert werden.

Die folgende Abbildung illustriert die Hauptkomponenten des Berechtigungsservice:

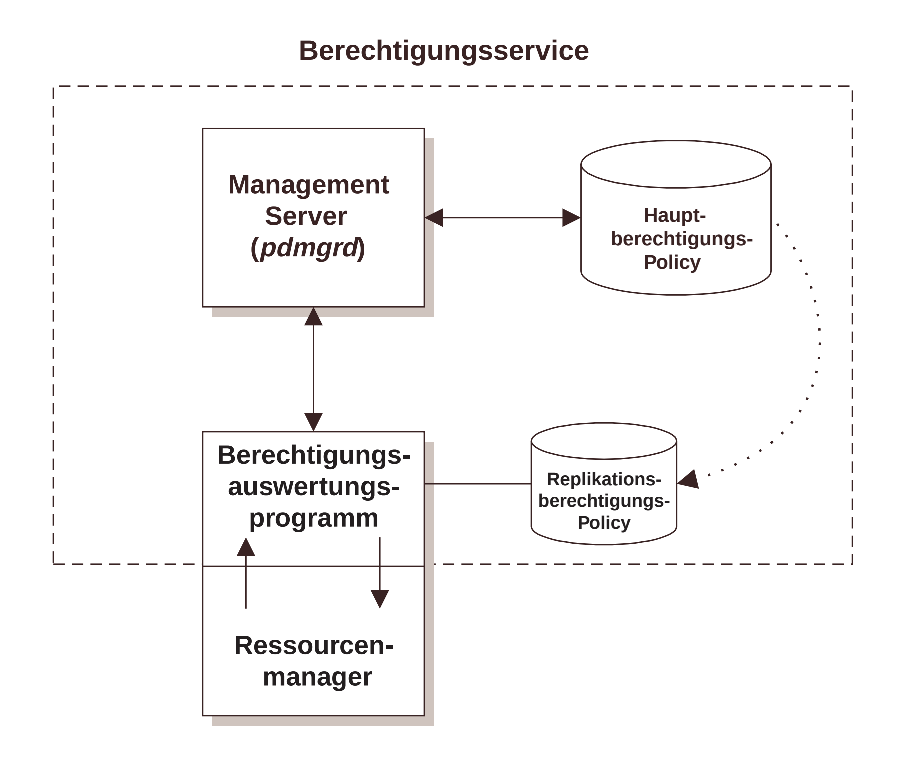



*Abbildung 3. Komponenten des Berechtigungsservice*

## Berechtigungsserviceschnittstellen

Der Berechtigungsservice verfügt über zwei Schnittstellen, an denen Interaktion stattfindet:

- **Verwaltungsschnittstelle** — Der Sicherheitsadministrator verwaltet die Sicherheits-Policy des Netzes mit Hilfe des Web Portal Manager (und/oder mit Hilfe des Dienstprogramms **pdadmin**), um Policy-Regeln (Schablonen) auf Netzressourcen anzuwenden und die Berechtigungen der Mitglieder der gesicherten Domäne zu registrieren.

  Der Web Portal Manager wendet diese Sicherheits-Policy-Daten über den Management Server auf die Hauptberechtigungs-Policy-Datenbank an.

  Diese Schnittstelle ist komplex und setzt detaillierte Kenntnisse des Objektbereichs, der Policy-Schablonen und der Berechtigungen voraus.

- **Berechtigungs-API** — Die Berechtigungs-API übergibt Anforderungen nach Berechtigungsentscheidungen vom Ressourcenmanager an das Berechtigungsauswertungsprogramm, das dann eine Empfehlung zurücksendet. Das Handbuch *Tivoli SecureWay Policy Director Authorization ADK Developer Reference* enthält Einzelheiten zu dieser API.

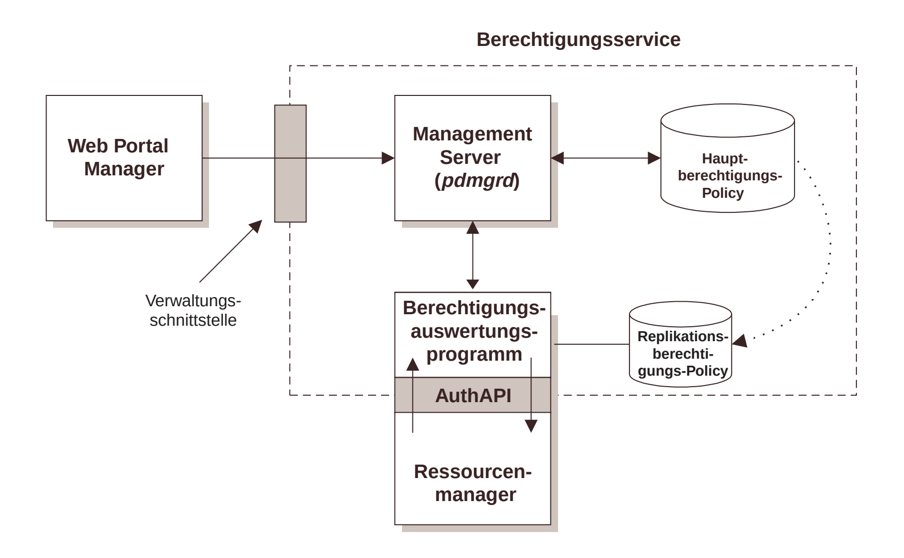



*Abbildung 4. Berechtigungsservice: Schnittstellen*

## Replikation für Skalierbarkeit und Leistung

Die Berechtigungsservicekomponenten können repliziert werden, um die Verfügbarkeit in einer Umgebung mit hohen Anforderungen zu verbessern.

Sie können die Hauptberechtigungs-Policy-Datenbank, die Policy-Regeln und Berechtigungsinformationen enthält, so konfigurieren, dass sie automatisch repliziert wird. Anwendungen, die den Berechtigungsservice aufrufen, haben zwei Möglichkeiten, auf diese Datenbankinformationen zu verweisen:

- Die Anwendung verwendet — wenn sie für eine reibungslose Zusammenarbeit mit dem Berechtigungsauswertungsprogramm konfiguriert ist — einen lokalen Cache der Datenbank.

  Die Datenbank wird für jede Anwendung, die den Berechtigungsservice im lokalen Cache-Modus verwendet, repliziert.

- Die Anwendung verwendet eine gemeinsame Replikation (Kopie), die die ferne Berechtigungsserverkomponente zwischenspeichert.

  Die Datenbank wird für jedes Exemplar des Berechtigungsservers repliziert. Viele Anwendungen können auf einen einzelnen Berechtigungsserver zugreifen.

Die Aktualisierungsbenachrichtigung vom Verwaltungsserver (sobald eine Änderung der Hauptberechtigungs-Policy-Datenbank vorgenommen wurde) löst den Cache-Prozess zum Aktualisieren aller Replikationen aus.

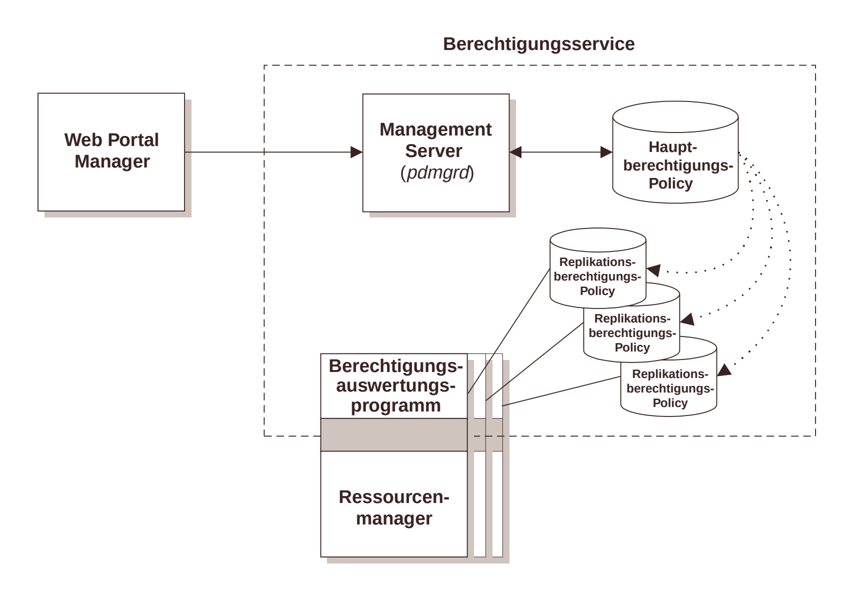



*Abbildung 5. Replizierte Berechtigungsservicekomponenten*

## Hinweise zur Leistung

- Neben den Aktualisierungsbenachrichtigungen direkt vom Verwaltungsserver prüfen die Anwendungsserver außerdem regelmäßig die Version der Hauptberechtigungs-Policy-Datenbank, um sicherzustellen, dass keine Aktualisierungsbenachrichtigung übersehen wird.

  Erreicht eine Aktualisierungsbenachrichtigung keinen Server, wird ein Protokolleintrag erstellt. In beiden Fällen wird durch einen Wiederholungsmechanismus sichergestellt, dass die Aktualisierung in Zukunft erfolgt.

- Die zwischengespeicherten Policy-Informationen bewirken eine hohe Systemleistung. Wenn beispielsweise WebSEAL eine Berechtigungsprüfung durchführt, wird die Policy-Schablone in der eigenen zwischengespeicherten Version der Datenbank überprüft. WebSEAL muss nicht auf das Netz zugreifen, um diese

Informationen aus der Hauptdatenbank abzurufen. Das Ergebnis sind sehr schnelle Antwortzeiten (Leistung) bei Berechtigungsprüfungen.

- Einzelne Berechtigungsergebnisse werden vom aufrufenden Anwendungsserver nicht zwischengespeichert.

# Implementieren einer Netzsicherheits-Policy

Die Sicherheits-Policy für eine gesicherte Domäne wird durch die Steuerung der Benutzer- und Gruppenmitgliedschaft in der Domäne und durch Anwenden von Regeln, so genannte ACL-Policies (ACL = Access Control List, Zugriffssteuerungsliste) und POP-Policies (POP = Protected Object Policies, Policies für geschützte Objekte), auf Ressourcen, die geschützt werden müssen, festgelegt. Der Berechtigungsservice führt diese Policies durch, indem die Berechtigungen eines Benutzers mit den Berechtigungen in der Policy, die der angeforderten Ressource zugeordnet ist, verglichen werden. Die resultierende Empfehlung wird an den Ressourcenmanager übermittelt, der die Antwort auf die ursprüngliche Anforderung abschließt.

## Definieren der Netzsicherheits-Policy

Der Berechtigungsservice verwendet eine zentrale Datenbank, die alle Ressourcen in der gesicherten Domäne und die ACL- und POP-Policies, die den einzelnen Ressourcen zugeordnet sind, enthält. Diese Hauptberechtigungs-Policy-Datenbank und die Benutzerregistrierungsdatenbank (mit Benutzer- und Gruppenkonten) sind die Hauptkomponenten für die Definition einer Netzsicherheits-Policy.

Zusammenfassend ausgedrückt steuert eine Netzsicherheits-Policy folgendes:

1. Welche Benutzer und Gruppen Mitglied in der gesicherten Domäne sein können

   Diese Informationen werden in der Benutzerregistrierungsdatenbank verwaltet.

2. Die Sicherungsstufe für alle Objekte in der gesicherten Domäne

   Diese Informationen werden in der Hauptberechtigungs-Policy-Datenbank verwaltet.

## Geschützter Objektbereich

Der geschützte Objektbereich ist eine hierarchische Darstellung von Ressourcen, die zu einer gesicherten Domäne gehören. Die Objekte in dem hierarchischen Objektbereich stellen die tatsächlichen Netzressourcen dar.

- **Systemressource** — Die tatsächliche physische Datei oder Anwendung.
- **Geschütztes Objekt** — Die logische Darstellung einer tatsächlichen Systemressource, die der Berechtigungsservice, Web Portal Manager und andere Policy Director-Verwaltungsdienstprogramme verwenden.

Objekten im Objektbereich können Policy-Schablonen zugeordnet werden, um den Schutz der Ressource zu gewährleisten. Der Berechtigungsservice trifft Berechtigungsentscheidungen anhand dieser Schablonen.

Policy Director verwendet folgende Objektbereichskategorien:

- **Webobjekte**

  Hierbei handelt es sich um alle Objekte, die mit einer HTTP-URL-Adresse aufgerufen werden können. Hierzu gehören statische Webseiten und dynamische URL-Adressen, die in Datenbankabfragen oder in eine andere Anwendungsart konvertiert werden.

- **Policy Director-Verwaltungsobjekte**

  Diese Objekte stellen die Verwaltungsaktivitäten dar, die über Web Portal Manager ausgeführt werden können. Die Objekte stellen die erforderlichen Tasks zum Definieren von Benutzern und Sicherheits-Policies dar. Policy Director unterstützt das Delegieren von Verwaltungsaktivitäten und kann die Möglichkeit eines Administrators, eine Sicherheits-Policy zu definieren, auf einen Teilbereich des Objektbereichs beschränken.

- **Benutzerdefinierte Objekte**

  Diese Objekte stellen benutzerdefinierte Tasks oder Netzressourcen dar, die durch Anwendungen mit Hilfe des Berechtigungsservice über die Berechtigungs-API geschützt werden.

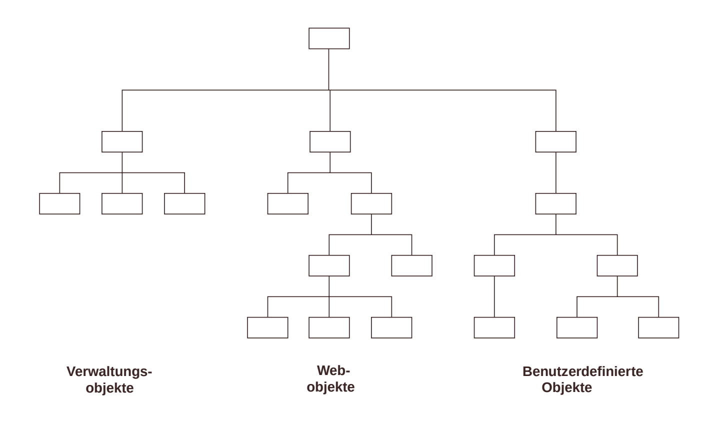



*Abbildung 6. Geschützter Objektbereich von Policy Director*

## ACL- und POP-Policies definieren und anwenden

Sicherheitsadministratoren schützen Systemressourcen durch Definition von Regel, so genannte ACL- und POP-Policies, und durch Anwenden dieser Policies auf die Objektdarstellungen dieser Ressourcen in dem Objektbereich.

Der Berechtigungsservice trifft Berechtigungsentscheidungen anhand der Policies, die auf diese Objekte angewendet werden. Wenn eine angeforderte Operation für ein geschütztes Objekt zugelassen wird, implementiert die Anwendung, die für die Ressource verantwortlich ist, diese Operation.

Eine Policy kann die Zugriffsschutzparameter von vielen Objekten festlegen. Jede Änderung wirkt sich auf alle Objekte, denen die Schablone zugeordnet ist, aus.

## Explizite und übernommene Policy

Policy kann explizit angewendet oder übernommen werden. Der geschützte Objektbereich von Policy Director unterstützt die Übernahme von ACL- und POP-Policy-Attributen. Diese Tatsache ist für den Sicherheitsadministrator, der den Objektbereich verwaltet, von großer Bedeutung. Der Administrator muss explizite Policies nur an den Punkten in der Hierarchie anwenden, an denen sich die Regeln ändern müssen.

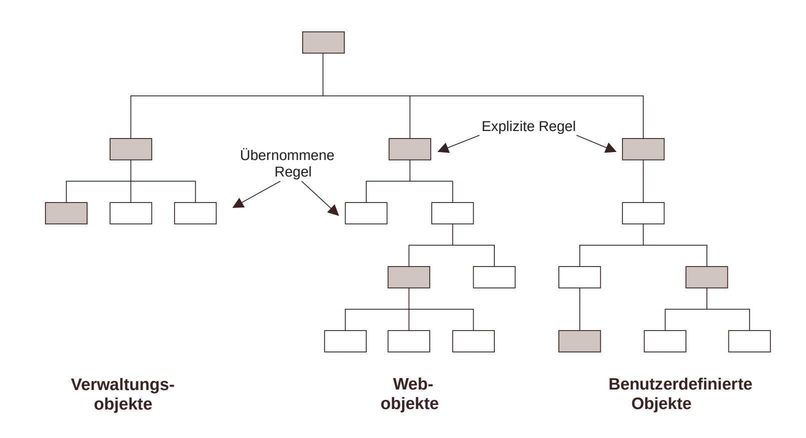



*Abbildung 7. Explizite und übernommene Policies*

Beispiele für Policy-Arten:

- Fest codierte Regeln
- Externe Berechtigungsfähigkeit
- Spezielle gesicherte Kennzeichnung
- Zugriffssteuerungslisten (ACLs)

## Zugriffssteuerungsliste (ACL)

Eine ACL-Policy (ACL = Access Control List, Zugriffssteuerungsliste) besteht aus einer Gruppe von Steuerangaben (Berechtigungen), die die Bedingungen angeben, die zum Ausführen bestimmter Operationen für eine Ressource erforderlich sind. ACL-Policy-Definitionen sind wichtige Bestandteile der Sicherheits-Policy für die gesicherte Domäne. ACL-Policies drücken den im geschützten Objektbereich dargestellten Ressourcen die Sicherheitsstandards einer Organisation auf.

Eine ACL-Policy steuert folgendes:

1. Welche Operationen für eine Ressource ausgeführt werden können
2. Wer diese Operationen ausführen kann

Eine ACL-Policy besteht aus mindestens einem Eintrag, der Benutzer- und Gruppenbezeichnungen und ihre spezifischen Berechtigungen enthält.

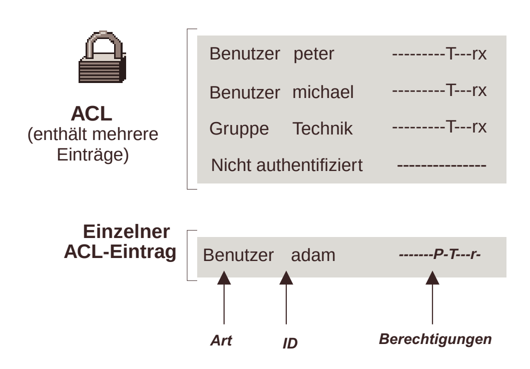



*Abbildung 8. ACL-Policy*

## POP-Policies

ACL-Policies stellen dem Berechtigungsservice Informationen zur Verfügung, mit denen eine positive oder eine negative Entscheidung bezüglich einer Zugriffsanforderung für ein geschütztes Objekt und für die Ausführung von Operationen mit diesem Objekt getroffen werden kann. POP-Policies (POP = Protected Object Policies, Policies für geschützte Objekte) enthalten zusätzliche Bedingungen für die Anforderung, die zusammen mit der positiven Entscheidung zur ACL-Policy vom Berechtigungsservice zurück an Policy Director Base und den Ressourcenmanager (z. B. WebSEAL) gesendet werden. Policy Director und der Ressourcenmanager sind für die Durchsetzung der POP-Bedingungen zuständig.

In den folgenden Tabellen sind die verfügbaren Attribute für eine POP-Policy aufgeführt:

| **Erzwungen durch Policy Director Base** | |
|---|---|
| **POP-Attribut** | **Beschreibung** |
| **Name** | Name der Policy. Dies wird der <*POP-Name*> in den **pdadmin pop**-Befehlen. |
| **Beschreibung** | Beschreibender Text für die Policy. Erscheint im **pop show**-Befehl. |
| **Warnungsmodus** | Methode zum Testen von ACL- und POP-Policies für Administratoren. |
| **Prüfungsstufe** | Gibt die Art der Prüfung an: Alle, Keine, Zulassen, Verweigern, Fehler. |
| **Zugriffszeit** | Tages- und Zeitangaben für einen erfolgreichen Zugriff auf ein geschütztes Objekt. |

| **Erzwungen durch Ressourcenmanager (z. B. WebSEAL)** | |
|---|---|
| **POP-Attribut** | **Beschreibung** |
| **Sicherungsstufe** | Gibt den Grad des Datenschutzes an: Keine, Integrität, Zugriffscode. |
| **Policy für IP-Endpunkt-Authentifizierungsmethode** | Gibt Authentifizierungsanforderungen für den Zugriff von externen Netzen an. |

## Policy-Verwaltung: Web Portal Manager

Web Portal Manager ist eine webbasierte Grafikanwendung, mit der die Sicherheits-Policy in einer gesicherten Domäne von Policy Director verwaltet wird. Das Befehlszeilendienstprogramm **pdadmin** verfügt über dieselben Verwaltungsfähigkeiten wie Web Portal Manager. Hinzu kommen viele Befehle, die Web Portal Manager nicht unterstützt.

Über Web Portal Manager (oder **pdadmin**) können Sie die Benutzerregistrierungsdatenbank, die Hauptberechtigungs-Policy-Datenbank und die Policy Director-Server verwalten. Außerdem können Sie Benutzer/Gruppen hinzufügen und löschen und ACL- und POP-Policies auf Netzobjekte anwenden.

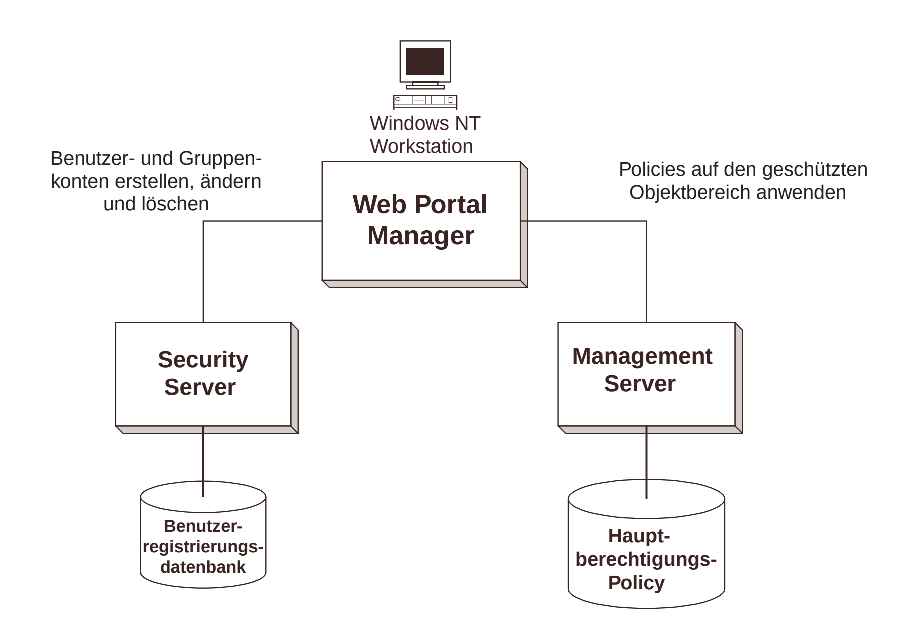



*Abbildung 9. Web Portal Manager: Verwaltung der Sicherheits-Policy*

## Die Schritte des Berechtigungsprozesses

Die folgende Abbildung illustriert den vollständigen Berechtigungsprozess:

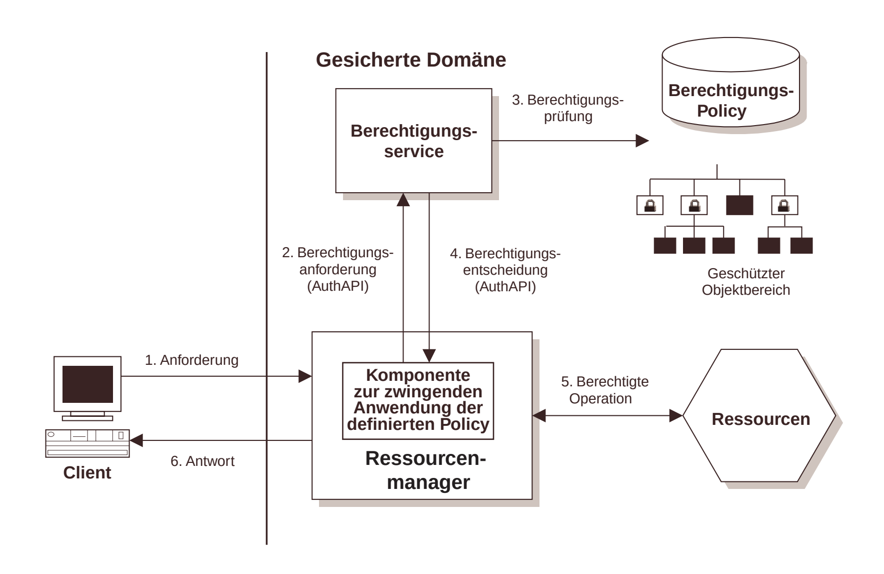



*Abbildung 10. Policy Director-Berechtigungsprozess*

1. Eine authentifizierte Client-Anforderung für eine Ressource wird an den Ressourcenmanagerserver weitergeleitet und durch die Komponente zur zwingenden Anwendung der definierten Policy abgefangen.

   Der Ressourcenmanager kann WebSEAL (für HTTP-, HTTPS-Zugriff) oder eine Anwendung eines anderen Herstellers sein.

2. Die Komponente zur zwingenden Anwendung der definierten Policy verwendet die Berechtigungs-API (siehe „Policy Director-Berechtigungs-API” auf Seite 35), um den Berechtigungsservice für eine Berechtigungsentscheidung aufzurufen.

3. Der Berechtigungsservice führt eine Berechtigungsprüfung für die Ressource durch, die als Objekt im geschützten Objektbereich dargestellt ist. Basis-POP-Policies werden als erstes geprüft. Dann wird die dem Objekt zugeordnete ACL-Policy mit der Berechtigung des Clients verglichen. Anschließend werden die durch den Ressourcenmanager erzwungenen POP-Policies überprüft.
4. Die positive oder negative Entscheidung für die Anforderung wird (über die Komponente zur zwingenden Anwendung der definierten Policy) als Empfehlung an den Ressourcenmanager zurückgesendet.
5. Wenn die Anforderung zugelassen wird, übergibt der Ressourcenmanager die Anforderung weiter an die für die Ressource zuständige Anwendung.
6. Der Client empfängt die Ergebnisse der angeforderten Operation.

## Policy Director-Berechtigungs-API

Mit Hilfe der Policy Director-Berechtigungs-API (API = Authorization Application Programming Interface, Anwendungsprogrammierschnittstelle) können Policy Director-Anwendungen und Anwendungen anderer Hersteller Berechtigungsentscheidungen vom Berechtigungsservice anfordern.

Die Berechtigungs-API ist die Schnittstelle zwischen dem Ressourcenmanager (der die Berechtigungsprüfung anfordert) und dem Berechtigungsservice. Die Berechtigungs-API gestattet der Anwendung, die die Policy umsetzt, eine Berechtigungsentscheidung anzufordern, schirmt die Anwendung jedoch von der Komplexität der eigentlichen Entscheidungsfindung ab.

Die Berechtigungs-API stellt ein Standardprogrammierungsmodell für die Codierung von Berechtigungsanforderungen und -entscheidungen zur Verfügung. Die Berechtigungs-API ermöglicht Ihnen, Standardaufrufe an den zentral verwalteten Berechtigungsservice von einer beliebigen herkömmlichen oder neu entwickelten Anwendung aus durchzuführen.

Die Berechtigungs-API kann in zwei Modusarten verwendet werden:

- **Ferner Cache-Modus**

  In diesem Modus wird die API so initialisiert, dass der (ferne) Authorization Server (**pdacld**) aufgerufen wird, um Berechtigungsentscheidungen für die Anwendung zu treffen. Der Authorization Server verwaltet einen eigenen Cache mit der Replikation (Kopie) der Berechtigungs-Policy-Datenbank. Dieser Modus wird für die Bearbeitung von Berechtigungsanforderungen von Anwendungs-Clients empfohlen.

  (Siehe „Berechtigungs-API: Ferner Cache-Modus" auf Seite 38.)

- **Lokaler Cache-Modus**

  In diesem Modus wird die API so initialisiert, dass eine lokale Replikation (Kopie) der Berechtigungsdatenbank für die Anwendung heruntergeladen und verwaltet wird. Der lokale Cache-Modus bewirkt einen besseren Durchsatz, weil die Anwendung alle Berechtigungsentscheidungen lokal und nicht über ein Netz trifft. Der Systemaufwand für die Datenbankreplikation und die erforderlichen Sicherheitsvorkehrungen für diesen Modus machen ihn jedoch zur optimalen Auswahl für gesicherte Anwendungsserver, wie z. B. WebSEAL.

  (Siehe „Berechtigungs-API: Lokaler Cache-Modus" auf Seite 40.)

Einer der Hauptvorteile der Berechtigungs-API liegt darin, dass dem Benutzer die Komplexität des Berechtigungsservicemechanismus an sich erspart bleibt. Verwaltung, Zwischenspeicherung, Replikation, Berechtigungsformate und Authentifizierungsmethoden bleiben hinter der Berechtigungs-API verdeckt.

Die Berechtigungs-API arbeitet außerdem unabhängig von der zugrundeliegenden Sicherheitsinfrastruktur, dem Berechtigungsformat und dem Prüfmechanismus. Die Berechtigungs-API macht es möglich, eine Berechtigungsprüfung anzufordern und eine einfache Empfehlung "Ja" oder "Nein" zu erhalten. Die Details der Berechtigungsprüfung bleiben dem Benutzer verborgen.

## Verwendung der Berechtigungs-API: Zwei Beispiele

Anwendungen eines anderen Herstellers können mit Hilfe der Berechtigungs-API Zugriffssteuerung für sehr spezifische und spezielle Prozesse ausführen.

**Beispiel 1:**

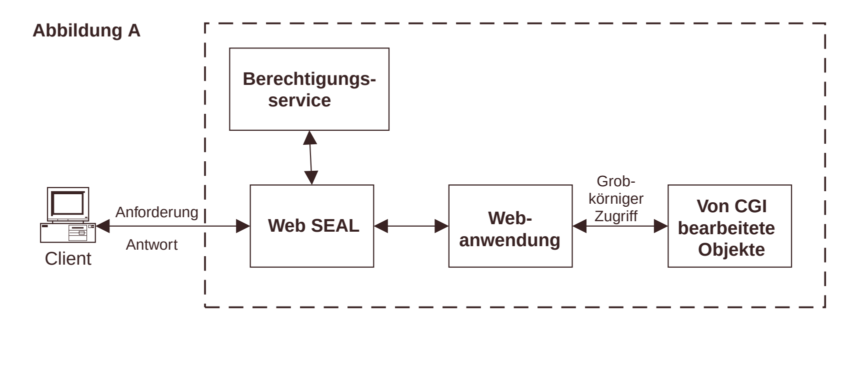
Eine grafische Benutzerschnittstelle kann entworfen werden, die Knöpfe gemäß den Ergebnissen der Berechtigungsprüfung dynamisch als aktiv oder inaktiv anzeigt.

**Beispiel 2:**

Eine weitere Verwendungsmöglichkeit der Berechtigungs-API wird in der folgenden Abbildung dargestellt, die eine Anforderung einer CGI-Transaktion durch eine Webanwendung zeigt.

Die Berechtigung der niedrigsten Stufe, in Abb. A dargestellt, beinhaltet eine Zugriffssteuerung der Art “alles oder nichts” für die URL-Adresse. Diese grobkörnige Berechtigungsstufe bestimmt lediglich, ob der Client das CGI-Programm ausführen kann. Wenn der Zugriff für die CGI-Anwendung zulässig ist, steht den Ressourcen, die von der CGI-Anwendung bearbeitet werden, keine weitere Steuerung zur Verfügung.

In Abb. B wurden Zugriffssteuerungen für Ressourcen definiert, die das CGI-Programm bearbeitet. Die Webanwendung ist so konfiguriert, dass sie die Berechtigungs-API verwendet. Jetzt kann das CGI-Programm den Berechtigungsservice aufrufen, um Berechtigungsentscheidungen für die bearbeiteten Ressourcen zu treffen — Grundlage hierfür ist die Identität des anfordernden Clients.



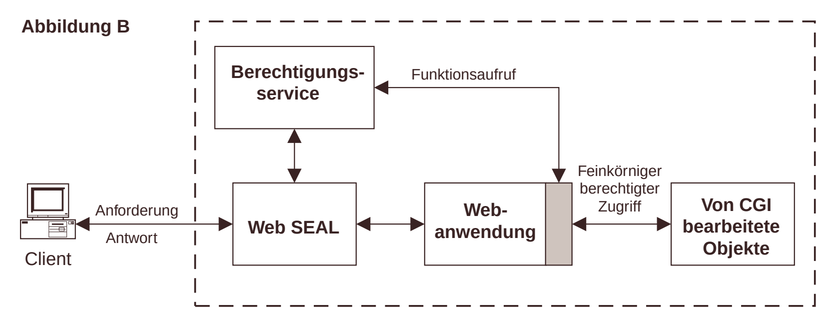




*Abbildung 11. Beispielverwendung der Berechtigungs-API*

## Berechtigungs-API: Ferner Cache-Modus

Im fernen Cache-Modus verwenden Anwendungen die Funktionsaufrufe, die die Berechtigungs-API zur Verfügung stellt, um mit dem (fernen) Authorization Server (**pdacld**) zu kommunizieren. Der Authorization Server fungiert als Auswertungsprogramm für die Berechtigungsentscheidungsfindung und verwaltet eine eigene Replikation (Kopie) der Berechtigungs-Policy-Datenbank.

Der Authorization Server trifft eine Entscheidung und gibt über die API eine Empfehlung an die Anwendung zurück. Der Server kann auch einen Protokolleintrag schreiben, der die Details der Berechtigungsentscheidungsanforderung enthält.

In der gesicherten Domäne muss ein Berechtigungsserver aktiv sein. Der Authorization Server kann sich auf derselben Maschine wie die Anwendung oder auf einer anderen Maschine befinden. Sie können den Authorization Server auch auf mehreren Maschinen in einer gesicherten Domäne installieren, um eine hohe Verfügbarkeit zu erreichen. Die Berechtigungs-API führt eine transparente Überbrückung durch, wenn ein bestimmter Authorization Server ausfällt.

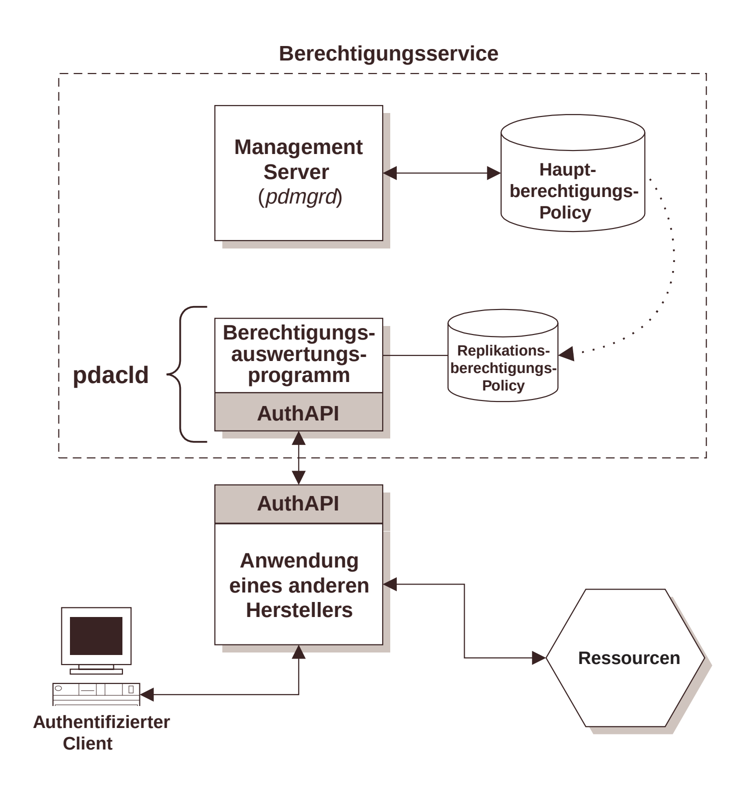



*Abbildung 12. Berechtigungs-API: Ferner Cache-Modus*

## Berechtigungs-API: Lokaler Cache-Modus

Im lokalen Cache-Modus lädt die API eine Replikation der Berechtigungs-Policy-Datenbank auf das lokale Dateisystem der Anwendung herunter und verwaltet sie dort. Sie führt alle Berechtigungsentscheidungen im Speicher durch, was eine verbesserte Leistung und Zuverlässigkeit bewirkt.

Sie müssen alle Anwendungen, die die Berechtigungs-API im lokalen Cache-Modus verwenden, manuell im Berechtigungsservice registrieren. Der Verwaltungsserver muss die Position jeder Berechtigungs-API-Anwendung im lokalen Cache-Modus kennen, damit er die Replikation der zugeordneten Berechtigungs-Policy-Datenbank aktualisieren kann.

Die lokale Replikation bleibt während der Aufrufe der Anwendung unverändert. Wenn die API im Replikationsmodus startet, wird die Hauptberechtigungs-Policy-Datenbank auf Aktualisierungen überprüft, die seit der Erstellung der lokalen Replikation (Kopie) aufgetreten sein können.

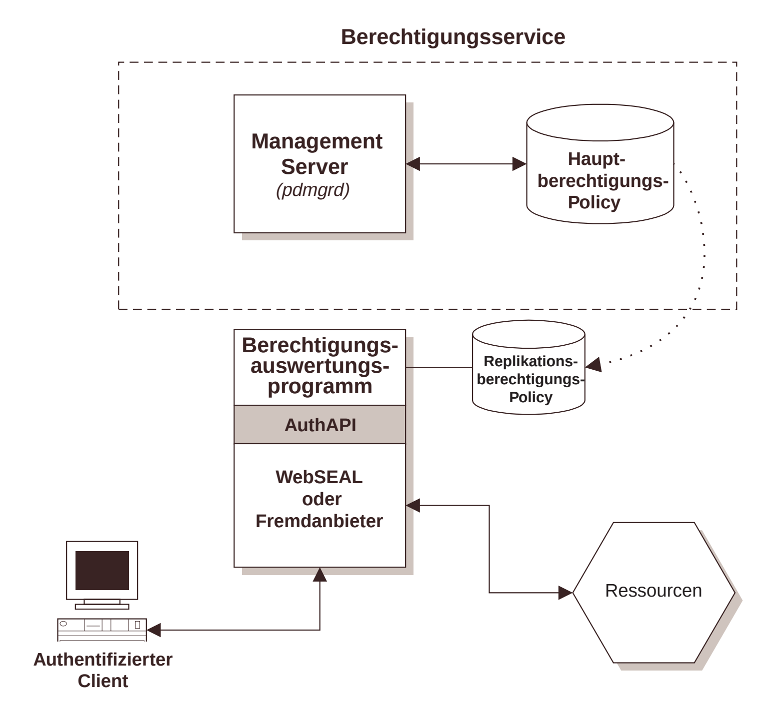



*Abbildung 13. Berechtigungs-API: Lokaler Cache-Modus*

## Externe Berechtigungsfähigkeit

In einigen Fällen können die Policy Director-Standard-Policy-Implementierungen (Zugriffssteuerungslisten und POP-Policies) unter Umständen nicht allen Berechtigungsregeln Ausdruck verleihen, die die Sicherheits-Policy eines Unternehmens erforderlich macht. Policy Director verfügt daher über eine optionale externe Berechtigungsfähigkeit, die alle zusätzlichen Berechtigungsanforderungen erfüllen soll.

Der externe Berechtigungsservice ermöglicht Ihnen, zusätzliche Berechtigungssteuerelemente und -bedingungen, die durch ein separates (externes) Berechtigungsservicemodul vorgegeben werden, anzugeben.

## Berechtigungsservice erweitern

Die externe Berechtigungsfähigkeit wird automatisch in den Berechtigungsservice von Policy Director integriert. Wenn Sie einen externen Berechtigungsservice konfigurieren, nimmt der Berechtigungsservice von Policy Director die Zugriffsentscheidungspfade einfach in seinen Prüfprozess auf.

Anwendungen, die den Berechtigungsservice nutzen (z. B. WebSEAL und alle Anwendungen, die die Berechtigungs-API verwenden) haben Vorteile von der zusätzlichen, aber nahtlosen Aufnahme eines konfigurierten externen Berechtigungsservice. Alle Erweiterungen der Sicherheits-Policy, die durch einen externen Berechtigungsservice erfolgen, sind für diese Anwendungen transparent und erfordern keine Änderung der Anwendungen.

Der externe Berechtigungsservice gestattet die vollständige Integration des vorhandenen Sicherheitsservice eines Unternehmens. Ein externer Berechtigungsservice bewahrt die Anfangsinvestitionen eines Unternehmens in Datenschutzmethoden, indem herkömmliche Server in den Prozess der Berechtigungsentscheidungsfindung von Policy Director integriert werden können.

## Bedingungen mit Ressourcenanforderungen verknüpfen

Mit Hilfe eines externen Berechtigungsservice können spezifischere Bedingungen oder systemspezifische Nebeneffekte mit einem erfolgreichen oder nicht erfolgreichen Zugriffsversuch verknüpft werden.

Beispiele für mögliche Bedingungen:

- Die Aufzeichnung des erfolgreichen oder nicht erfolgreichen Zugriffsversuchs durch einen externen Prüfungsmechanismus auslösen
- Aktive Überwachung des Zugriffsversuchs und Auslösen eines Alerts oder Alarmsignals sobald unzulässige Vorgehensweise festgestellt wird
- Rechnungsstellungs- und Mikrozahlungstransaktionen
- Zugriffsquoten für eine geschützte Ressource festlegen

## Berechtigungsauswertungsprozess

Eine Berechtigungsentscheidung, an der ein externer Berechtigungsserver beteiligt ist, wird wie folgt getroffen:

1. Wird im Laufe einer Zugriffsentscheidung eine Auslöserbedingung erfüllt, werden die für diese Bedingung konfigurierten externen Berechtigungsservices nacheinander aufgerufen, um ihre eigenen externen Berechtigungsbedingungen zu prüfen.

   Der Aufruf des externen Berechtigungsservice erfolgt unabhängig davon, ob der Policy Director Berechtigungsservice dem Benutzer die erforderliche Berechtigung erteilt oder nicht.

2. Jeder externe Berechtigungsservice gibt eine der folgenden Entscheidungen zurück: Zulässig, verweigert oder neutral.

   Bei einer neutralen Entscheidung hat der externe Berechtigungsservice festgestellt, dass er für den Entscheidungsprozess nicht erforderlich ist, so dass er nicht daran teilnimmt.

3. Jede Entscheidung des externen Berechtigungsservice wird gemäß ihrer Bedeutung in dem Prozess gewichtet.

   Die Gewichtung einzelner externer Berechtigungsservices wird beim Laden des Service-Plug-Ins konfiguriert.

4. Alle Ergebnisse der Berechtigungsentscheidung werden summiert und mit der Entscheidung des Policy Director-Berechtigungsservice kombiniert. Die resultierende Entscheidung wird an den Aufrufenden zurückgegeben.

### Beispiel

Die folgende Abbildung illustriert eine Berechtigungsentscheidung, an der ein WebSEAL-Server und ein externer Berechtigungsservice beteiligt sind.

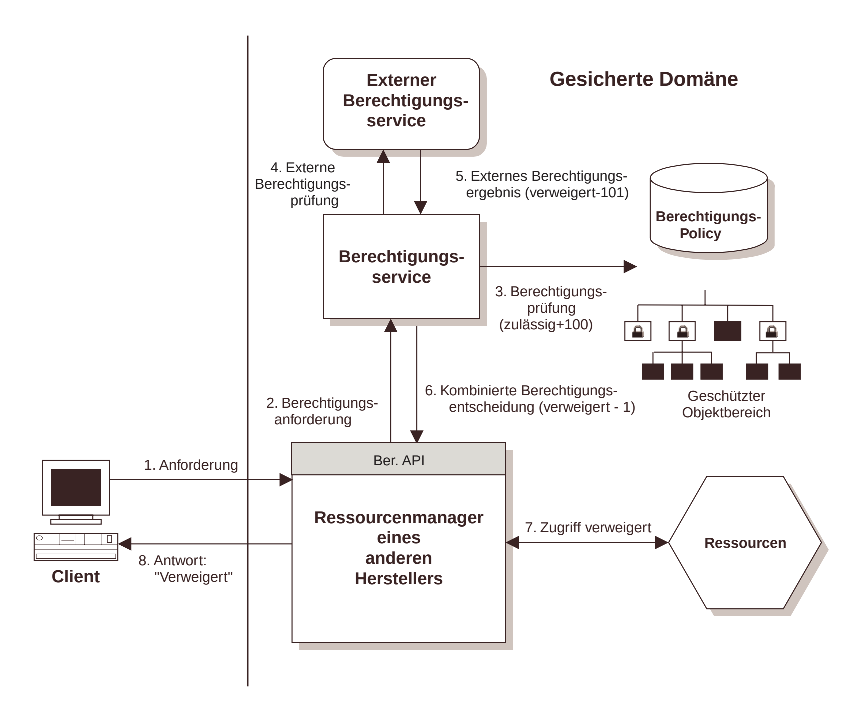



*Abbildung 14. Externer Berechtigungsservice mit WebSEAL*

In diesem Beispiel dient der externe Berechtigungsservice dazu, eine Einschränkung bezüglich der Verwendungshäufigkeit der Druckerressource mit Fotoqualität festzulegen.

Die Serviceimplementierung legt eine Begrenzung der Anzahl Jobs fest, die eine Person wöchentlich an diesen Drucker übergeben kann. Der Fotodruckerressource wurde eine Auslöserbedingung des externen Berechtigungsservice zugeordnet, so dass der externe Berechtigungsservice bei jedem Zugriff auf den Fotodrucker aufgerufen wird.

Der externe Berechtigungsservice wurde mit der Standardentscheidungsgewichtung 101 geladen, die im Bedarfsfall alle Entscheidungen des Policy Director-Berechtigungsservice außer Kraft setzt.

1. Der WebSEAL-Server empfängt eine Anforderung von einem Client für den Zugriff auf eine Online-Fotodruckerressource. Der Client gehört zur entsprechenden Gruppe ″GraphicArtists″, so dass er normalerweise berechtigt ist, Jobs an den Drucker zu übergeben.
2. Der WebSEAL-Server fragt zunächst im Policy Director-Berechtigungsservice nach, ob der anfordernde Benutzer über eine Berechtigung für die Übergabe von Jobs an den Drucker verfügt.
3. Der Policy Director-Berechtigungsservice überprüft die Zugriffsberechtigungen für das angeforderte Zielobjekt und vergleicht diese mit den Berechtigungen des anfordernden Benutzers:

   ```
   Gruppe GraphicArtists rx
   ```

   In der ACL der Druckerressource gestattet die Berechtigung “x” allen Benutzern der Gruppe ″GraphicArtists″ einen Zugriff auf die Ressource. Daher erteilt der Policy Director-Berechtigungsservice dem Benutzer die Berechtigung für die Übergabe des Jobs.
4. Da auf die Fotodruckerressource zugegriffen wird und diesem Objekt eine Auslöserbedingung des externen Berechtigungsservice zugeordnet ist, erfolgt außerdem eine Anforderung an den externen Berechtigungsservice, der für diese Auslöserbedingung konfiguriert ist.

   Der externe Berechtigungsservice empfängt alle Zugriffsentscheidungsinformationen, die mit der ursprünglichen Zugriffsentscheidungsprüfung durch WebSEAL übergeben wurden.
5. Der externe Berechtigungsservice prüft die Aufzeichnung der vorherigen Zugriffe durch diesen Benutzer. Hat der anfordernde Benutzer seine wöchentliche Quote nicht überschritten, wird eine neutrale Zugriffsentscheidung zurückgegeben.

   Daraus folgt, dass der externe Berechtigungsservice die Anforderung nicht beachtet und sich nicht an der Zugriffsentscheidung beteiligt, da seine Bedingungen für eine Zugriffsverweigerung nicht erfüllt wurden.

Hat der Benutzer jedoch seine Quote überschritten, gibt der externe Berechtigungsservice die Entscheidung “Zugriff verweigert” zurück.

In diesem Beispiel wird vorausgesetzt, dass der anfordernde Benutzer seine Quote überschritten hat und dass der externe Berechtigungsservice dies feststellt und die Entscheidung “Zugriff verweigert” trifft.

6. Der Policy Director-Berechtigungsservice empfängt das Ergebnis “Zugriff verweigert” vom externen Berechtigungsservice. Dann wird diese Entscheidung mit dem Standardgewichtungswert 101 des externen Berechtigungsservice gewichtet.

   Das Ergebnis der Entscheidung des externen Berechtigungsservice und das Ergebnis der Entscheidung des Policy Director-Berechtigungsservice werden kombiniert. Das Endergebnis lautet “Zugriff verweigert”, weil das Ergebnis des externen Berechtigungsservice (-101) das Ergebnis des Policy Director-Berechtigungsservice (100) übertrifft.

7. Der WebSEAL-Server weist die Jobübergabe an die Fotodruckerressource zurück.

8. Der WebSEAL-Server sendet eine Antwort an den anfordernden Benutzer, um anzuzeigen, dass der Job zurückgewiesen wurde.

## Externen Berechtigungsservice implementieren

Für einen externen Berechtigungsservice sind zwei allgemeine Schritte erforderlich:

1. Schreiben eines Plug-In-Moduls für externen Berechtigungsservice mit einer Berechtigungsschnittstelle, auf die bei Berechtigungsentscheidungen verwiesen werden kann.

2. Registrieren des externen Berechtigungsservice in Policy Director, so dass Policy Director-Berechtigungs-Clients den Plug-In-Service während der Initialisierung laden können.

Durch das Registrieren des Service wird eine Auslöserbedingung für den Aufruf des externen Berechtigungsservice definiert. Wenn die Auslöserbedingung während einer Berechtigungsprüfung festgestellt wird, wird die Schnittstelle des externen Berechtigungsservers aufgerufen, um eine zusätzliche Berechtigungsentscheidung zu treffen.

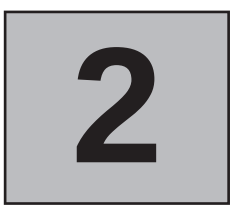
Weitere Informationen zur Implementierung eines externen Berechtigungsservice finden Sie im Handbuch *Tivoli SecureWay Policy Director Authorization API Developer Reference*.

## Implementierungsstrategien

Policy Director ermöglicht verschiedene Implementierungsarten für einen externen Berechtigungsservice:

- Der gesicherten Domäne kann eine beliebige Anzahl externer Berechtigungsserver hinzugefügt werden, um verschiedene Berechtigungsauswertungen durchzuführen. Jeder externe Berechtigungsservice wird in die einzelne Berechtigungs-API-Client-Anwendung im Lokalmodus geladen. Zu den Anwendungen, die externe Berechtigungsservices laden können, gehören WebSEAL (**webseald**), der Authorization Server (**PDAcld**), andere Policy Director-Server sowie alle vom Kunden erstellten Berechtigungsanwendungen.
- Berechtigungs-API-Clients im Fernmodus, die Berechtigungsentscheidungen vom Authorization Server anfordern, verwenden automatisch alle externen Berechtigungsservices, die der Authorization Server lädt.
- Für eine einzelne Auslöserbedingung können mehrere externe Berechtigungsservices aufgerufen werden. In diesem Fall werden die Ergebnisse jedes externen Berechtigungsservice entsprechend gewichtet; dann werden die Ergebnisse mit dem Ergebnis des Policy Director-Berechtigungsservice kombiniert.
- Auslöserbedingungen können für Objekte definiert werden (mit Hilfe eines POP-Policy-Auslösers), so dass jede Anforderung eines Objekts - unabhängig von der angeforderten Operation - einen Aufruf der externen Berechtigungsservices, die für den Auslöser konfiguriert sind, auslöst.

- Auslöserbedingungen können auch für die von einem Benutzer angeforderten Operationen definiert werden. Beispielsweise kann ein externer Berechtigungsservice ausgelöst werden, wenn ein Benutzer eine Schreiboperation für eine geschützte Ressource anfordert, aber nicht bei anderen Operationen. Dann ist es möglich, Operationsgruppen zu entwickeln, für die ein externer Berechtigungsservice oder eine Kombination mehrerer externer Berechtigungsservices gemäß der angeforderten Operationsgruppe ausgelöst wird.
- Die externen Berechtigungsservices werden als DLL-Module (DLL = Dynamically Loadable Library) implementiert. Dadurch wird die Entwicklung des externen Berechtigungsservice sehr vereinfacht. Es sind keine Anforderungen an einen fernen externen Berechtigungsservice erforderlich, und der Systemaufwand für den Aufruf entspricht dem Systemaufwand für einen Funktionsaufruf.
- Die Kombination aus Berechtigungs-API und externem Berechtigungsservice bietet eine in höchstem Maß erweiterbare und flexible Lösung für die Implementierung einer komplexen Sicherheits-Policy.



# Geschützten Objektbereich verwalten



Eine gesicherte Domäne von Policy Director enthält physische Ressourcen, die normalerweise einen bestimmten Schutz benötigen. Zu den Ressourcen gehören Dateien, Verzeichnisse und Druckerservices. Policy Director verwendet eine virtuelle Darstellung dieser Ressourcen, die als geschützter Objektbereich bezeichnet wird.

Ressourcen können geschützt werden, indem den Objektdarstellungen dieser Ressourcen ACL- und POP-Policies zugeordnet werden. Dieses Kapitel beschreibt den geschützten Objektbereich und wie Sie Erweiterungen des Objektbereichs erstellen können, um benutzer-
definierte Anwendungsanforderungen zu unterstützen.

Stichwortindex:



## Erläuterungen zum geschützten Objektbereich

Eine gesicherte Domäne von Policy Director enthält physische Ressourcen, die einen bestimmten Zugriffsschutz benötigen. Zu den Ressourcen gehören Dateien, Verzeichnisse, Netz-Ports, Anwendungen und Druckerservices.

Das Policy Director-Sicherheitsmodell beruht auf ACL- und POP-Policies, die einen sicheren Zugriffsschutz für diese Ressourcen gewährleisten. Eine Unternehmenssicherheits-Policy wird durch die angepassten ACL- und POP-Policies, die strategisch angewendet werden, für diese schutzbedürftigen Ressourcen implementiert. Der Policy Director-Berechtigungsservice trifft die Entscheidung, den Zugriff auf Ressourcen zu gestatten oder zu verweigern, anhand von Benutzerberechtigungen und anhand der spezifischen Berechtigungen und Bedingungen, die in den ACL- und POP-Policies festgelegt sind.

Damit ACL- und POP-Policies angewendet werden und damit der Berechtigungsservice seine Sicherheitsprüfungen ausführen kann, verwendet Policy Director eine virtuelle Objektdarstellung für Ressourcen der gesicherten Domäne, die als geschützter Objektbereich bezeichnet wird.

Ein Policy Director-Sicherheitsadministrator ordnet mit Hilfe des Web Portal Manager oder des Dienstprogramms **pdadmin** den logischen Objekten in dem Objektbereich ACL- und POP-Policies zu.

## Elemente des geschützten Objektbereichs

Der geschützte Objektbereich von Policy Director ist eine logische und hierarchische Darstellung von Ressourcen, die zu einer gesicherten Domäne gehören. Objekte in dem hierarchischen Objektbereich stellen tatsächliche physische Netzressourcen dar.

- **Systemressource** – Die tatsächliche physische Datei, der tatsächliche Netzservice oder die tatsächliche Anwendung
- **Geschütztes Objekt** – Die logische Darstellung einer tatsächlichen Systemressource, die der Berechtigungsservice, Web Portal Manager und andere Policy Director-Verwaltungsdienstprogramme verwenden

Der geschützte Objektbereich enthält zwei Objektarten:

- **Containerobjekte**

  Containerobjekte sind Strukturelemente, mit denen Sie eine aus begrenzten funktionalen Bereichen bestehende Hierarchie für den Objektbereich aufbauen können. Containerobjekte enthalten Ressourcenobjekte.

- **Ressourcenobjekte**

  Ressourcenobjekte sind die Darstellungen tatsächlicher Netzressourcen (z. B. Services, Dateien und Programme) in Ihrer gesicherten Domäne.



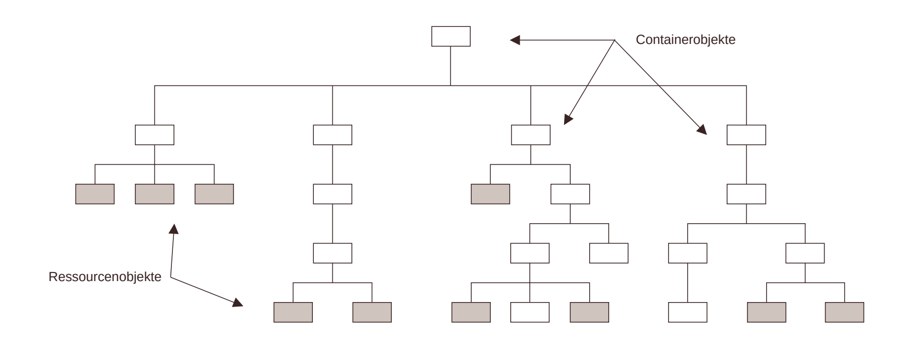



*Abbildung 15. Geschützter Objektbereich von Policy Director*

## Hierarchie des geschützten Objektbereichs

Die strukturelle Spitze oder der Anfang des geschützten Objektbereichs ist das **Stamm**containerobjekt (Root). Das Symbol für den **Stamm** ist der Schrägstrich (/).

An das **Stamm**objekt schließen sich folgende Objektbereichskategorien an:

- **Webobjekte (Container /WebSEAL)**

  Das WebSEAL-Containerobjekt ist der Stamm des logischen Webbereichs der gesicherten Domäne. Alle HTTP-Operationen sind für ein Objekt in dieser untergeordneten Baumstruktur berechtigt.

  Webobjekte sind alle Objekte, die mit einer URL-Adresse aufgerufen werden können. Hierzu gehören statische Webseiten und dynamische URL-Adressen, die in Datenbankabfragen oder in eine andere Anwendungsaufrufart durch ein Gateway zwischen Web und Anwendung konvertiert werden.

- **Policy Director-Verwaltungsobjekte (Container /Management)**

  Das Management-Containerobjekt ist der Stamm des logischen Bereichs, der alle Policy Director-Verwaltungsoperationen steuert. Verwaltungsobjekte stellen die Services dar, die zum Definieren von Benutzern und Gruppen und zum Festlegen der Sicherheits-Policy erforderlich sind. Diese Tasks können mit Web Portal Manager oder mit dem Dienstprogramm **pdadmin** ausgeführt werden.

  Der Bereich /Management ist wie folgt unterteilt:

  - Benutzerverwaltung (/Users)
  - Gruppenverwaltung (/Groups)
  - GSO-Verwaltung (/GSO)
  - Serververwaltung (/Server)
  - ACL-Policy (/ACL)
  - POP-Policy (/POP)

- Konfigurationsberechtigungssteuerung (/Config)
- Berechtigungssteuerung Dritter (/Action)
- Replikationssteuerung für Berechtigungsdatenbank (/Replica)

Policy Director unterstützt das Delegieren bestimmter Verwaltungsaktivitäten und kann die Möglichkeit eines Administrators, eine Sicherheits-Policy zu definieren, auf einen Teilbereich des Objektbereichs beschränken.

- **Benutzerdefinierte Objekte**

  Diese Objekte stellen benutzerdefinierte Tasks oder Netzressourcen dar, die durch Anwendungen eines anderen Herstellers, die über die Berechtigungs-API Aufrufe an den Policy Director-Berechtigungsservice durchführen, geschützt werden.

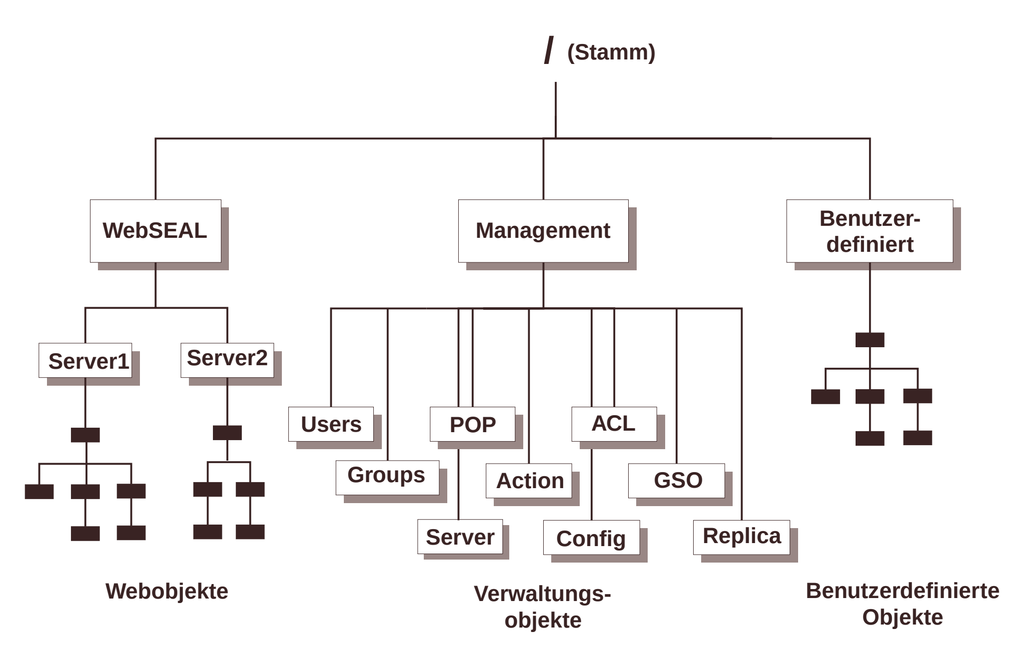



*Abbildung 16. Bereiche des geschützten Objektbereichs von Policy Director*

## Benutzerdefinierter Objektbereich für Anwendungen eines anderen Herstellers

Policy Director kann Berechtigungsservices für jedes Objekt einer Anwendung eines anderen Herstellers, das durch den geschützten Objektbereich definiert ist, zur Verfügung stellen.

Für jede Anwendung, die Policy Director verwendet, muss ein Bereich des Objektbereichs definiert werden. WebSEAL verfügt beispielsweise über einen eigenen Objektbereich (/WebSEAL). Policy Director speichert Verwaltungsobjekte im Objektbereich /Management.

Diese Objektbereiche erscheinen in einem Befehl **pdadmin objectspace list**:

```
pdadmin> objectspace list
       /WebSEAL
       /Management
```

Policy Director und Anwendungen eines anderen Herstellers führen Aufrufe an den Berechtigungsservice über die Berechtigungs-API durch. Für die Integration einer Anwendung eines anderen Herstellers in den Berechtigungsservice sind zwei Schritte erforderlich:

- Den Objektbereich für die Anwendung eines anderen Herstellers beschreiben
- Berechtigungen für alle Objekte, die geschützt werden müssen, anwenden

Optionale Container mit “benutzerdefinierten Objekten” sind Bereiche des geschützten Objektbereichs, in denen Sie Objekte für Anwendungen eines anderen Herstellers erstellen können. Bevor Sie neue Objekte hinzufügen können, müssen Sie einen neuen Objektbereichscontainer definieren.

# Datenbankobjektbereich definieren

Policy Director gestattet die Ausdehnung seiner Berechtigungs-services auf Objekte, die zu einem benutzerdefinierten Objektbereich Dritter gehören. Für die Integration eines Objektbereichs Dritter in Policy Director sind zwei Schritte erforderlich:

- Den Objektbereich für die Anwendung eines anderen Herstellers in Policy Director beschreiben
- ACL- und POP-Policies für alle Objekte, die geschützt werden müssen, anwenden

Der Befehl **pdadmin objectspace** gestattet eine einfache Erstellung von Bereichen im benutzerdefinierten Objektbereich und die Verwaltung der Objekte in diesen Bereichen. Mit diesem Befehl erstellte benutzerdefinierte Objektbereiche sind dynamisch, weil sie aktualisiert werden können, während Policy Director aktiv ist.

## Neues benutzerdefiniertes Containerobjekt erstellen

Mit den Befehlen **pdadmin objectspace** und **object** verwalten Sie benutzerdefinierte Objektbereiche. Der Befehl **objectspace** erstellt ein Containerartobjekt.

**Anmerkung:** Die Standardobjektbereiche von Policy Director (/WebSEAL und /Management) können nicht mit dem Befehl **pdadmin objectspace** gesteuert werden.

Syntax:

```
pdadmin> objectspace create <Name> <Beschreibung> <Art>
```

Der Objektbereich *Name* muss mit einem Schrägstrich (/) beginnen.

Die *Beschreibung* wird im Web Portal Manager angezeigt.

Die *Art* kann eine der folgenden Kategorien sein:

| Objektarten | |
|---|---|
| 0 – unbekannt | 9 – HTTP-Server |
| 1 – gesicherte Domäne | 10 – nicht vorhandenes Objekt |
| 2 – Datei | 11 – Containerobjekt |
| 3 – ausführbares Programm | 12 – Blattobjekt |
| 4 – Verzeichnis | 13 – Port |
| 5 – Junction | 14 – Anwendungscontainerobjekt |
| 6 – WebSEAL-Server | 15 – Anwendungsblattobjekt |
| 7 – nicht verwendet | 16 – Verwaltungsobjekt |
| 8 – nicht verwendet | 17 – nicht verwendet |

Die Kategorie ″Art″ verwendet Web Portal Manager nur zum Anzeigen eines entsprechenden Symbols mit dem Objekt.

Bei der Erstellung eines Objekts muss eine Art angegeben werden. Sie können eine entsprechende Kategorie auswählen oder die Art **0** für “unbekannt” verwenden.

Zum Beispiel:

```
pdadmin> objectspace create /Test-Space "Neuer Objektbereich" 14
pdadmin> objectspace list
       /WebSEAL
       /Management
       /Management/Users
       /Management/Groups
       /Test-Space
```

## Verwaltungshinweise:

- Für jede Anwendung eines anderen Herstellers sollte ein separater Objektbereich erstellt werden.
- Sie müssen den neuen Objektbereich definieren, bevor Sie Objekte hinzufügen können.
- Für den Stamm des Objektbereichs, der gleichzeitig mit der Definition des Objektbereichs erstellt wird, wird automatisch das Attribut **ispolicyattachable** festgelegt.

## Objekte erstellen und löschen

Sobald ein Objektbereich erstellt worden ist, können Sie ihn mit Objekten ausfüllen.

Verwenden Sie zum Verwalten von benutzerdefinierten Objekten den Befehl **pdadmin objects**.

```
pdadmin> object create <Name> <Beschreibung> <Art>
ispolicyattachable {yes|no}
```

Ein Objekt verfügt über folgende Felder:

| Argument | Beschreibung |
|---|---|
| **Name** | Dies ist die vollständig qualifizierte Position des Objekts im Objektbereich. Am Anfang steht ein vorhandener Objektbereichsname. |
| **Beschreibung** | Die Textbeschreibung des Objekts. |
| **Art** | Die Art des zu erstellenden Objekts. Verwendet Web Portal Manager zum Anzeigen eines entsprechenden Symbols. |
| **ispolicyattachable** | Zeigt an, ob dem Objekt eine POP-Policy zugeordnet werden kann. Wird “no” angegeben, übernimmt das Objekt die übergeordnete Policy. Wird verwendet, um zu erzwingen, dass Kindobjekte dieselbe Policy wie das Elter (übergeordnetes Objekt) verwenden. |

Zum Beispiel:

```
pdadmin> object create /Test-Space/folder1 "Ordner 1" 14
ispolicyattachable yes

pdadmin> object list /Test-Space
       folder1

pdadmin> object show /Test-Space/folder1
       Name: /Test-Space/folder1
              Beschreibung: Ordner 1
              Art: (Anwendungscontainerobjekt): 14
              Kann Policy zugeordnet werden: yes

pdadmin> object create /Test-Space/folder2 "Ordner 2" 14
ispolicyattachable no
```

```
pdadmin> object listandshow /Test-Space
       Name: folder1
              Beschreibung: Ordner 1
              Art: (Anwendungscontainerobjekt): 14
              Kann Policy zugeordnet werden: yes
       Name: folder2
              Beschreibung: Ordner 2
              Art: (Anwendungscontainerobjekt): 14
              Kann Policy zugeordnet werden: no

pdadmin> object delete /Test-Space/folder1
pdadmin> object list /Test-Space
       folder2
```

### Verwaltungshinweise:

- Kindobjekte werden nicht verschoben, wenn Sie den Namen des Elternobjekts ändern. Kindobjekte können daher ohne Elternobjekte gelassen werden. Wenn Sie den Namen eines Elternobjekts ändern, müssen Sie alle Kindobjekte verschieben.
- Wenn das Feld **ispolicyattachable** im Befehl **pdadmin object create** ausgelassen wird, geht das Dienstprogramm davon aus, dass Sie den Befehl **objectspace create** verwenden wollen. Es wird kein Objekt, sondern ein Objektbereich erstellt.

# 3

# ACL-Policies verwenden

Policy Director verwendet eine virtuelle Darstellung der Ressourcen in der gesicherten Domäne—den so genannten geschützten Objektbereich. Ressourcen können durch Definieren von speziellen Sicherheitsstrategien (Policy) und durch Verknüpfen dieser Strategien mit der Objektdarstellung dieser Ressourcen im geschützten Objektbereich geschützt werden.

Die Policy-Art, die festlegt, wer auf ein Objekt zugreifen kann und welche Operationen für das Objekt ausgeführt werden können, wird als **ACL-Policy** (ACL = Access Control List, Zugriffssteuerungsliste) bezeichnet. Die ACL-Policies unterstützen die Implementierung der Sicherheits-Policies eines Unternehmens für die Ressourcen der gesicherten Domäne.

Stichwortindex:

# Einführung in die ACL-Policy

Eine ACL-Policy (ACL = Access Control List, Zugriffssteuerungsliste) ist eine von Policy Director verwendete Methode, die feinkörnigen Zugriffsschutz für Ressourcen in der gesicherten Domäne zur Verfügung stellt.

Eine ACL-Policy ist eine Gruppe von Regeln oder Berechtigungen, die die Bedingungen angeben, die für die Ausführung einer Operation mit einem geschützten Objekt erforderlich sind. Eine ACL-Policy legt die Operationen fest, die für ein geschütztes Objekt zulässig sind, und listet die Personen (Benutzer und Gruppen) auf, die diese Operationen ausführen können.

- Benutzer- und Gruppenidentitäten sind in der Registrierungsdatenbank von Policy Director definiert.
- Der geschützte Objektbereich und ACL-Policies sind in der Hauptberechtigungsdatenbank definiert.

Jede ACL-Policy verfügt über einen eindeutigen Namen oder eine Bezeichnung. Jede ACL-Policy kann auf mindestens ein Objekt angewendet werden.

Eine ACL-Policy besteht aus mindestens einem **Eintrag**, der Benutzer- und Gruppenbezeichnungen und ihre spezifischen Berechtigungen enthält.

## ACL-Policy-Einträge

Eine ACL-Policy besteht aus mindestens einem Eintrag, der folgendes beschreibt:

- Die Namen von Benutzern und Gruppen, deren Zugriff auf das Objekt explizit gesteuert wird

- Die spezifischen Operationen, die für jeden Benutzer, für jede Gruppe oder Berechtigung zulässig sind
- Die spezifischen Operationen, die für die Sonderbenutzerkategorien **Beliebige andere** und **Nicht authentifiziert** zulässig sind

Ein **Benutzer** stellt eine authentifizierte Policy Director-Identität dar. Normalerweise stellen Benutzer Netzbenutzer oder Anwendungsserver dar.

Eine **Gruppe** besteht aus mindestens einem Benutzer. Ein Netzadministrator kann mit Hilfe von Gruppen-ACL-Einträgen auf einfache Weise mehreren Benutzern dieselben Berechtigungen zuordnen. Neue Benutzer in der gesicherten Domäne erlangen den Zugriff auf Objekte, indem Sie Mitglied der entsprechenden Gruppen werden. Auf diese Weise ist es nicht erforderlich, neue ACL-Einträge für jeden neuen Benutzer zu erstellen. Gruppen können Unternehmensbereiche oder Abteilungen in einer gesicherten Domäne darstellen. Gruppen sind auch beim Definieren von Berechtigungsklassen oder Funktionszuordnungen von Nutzen.

Benutzer und Gruppen werden übergreifend als **Definitionseinheiten** bezeichnet.

Benutzer- und Gruppeneinträge in ACLs werden mit Hilfe einer UUID (Universal Unique Identifier) gespeichert. Die UUID bietet zusätzliche Sicherheit für den Fall, in dem ein Benutzer oder eine Gruppe aus der Domäne gelöscht und dann unter demselben Domänennamen erneut erstellt wird. Beispiel: Auch wenn ein neuer Benutzer denselben Namen wie der gelöschte Benutzer hat, ordnet Policy Director diesem Benutzer eine neue UUID zu. Da die UUID neu ist, werden dem neuen Benutzer keine Berechtigungen durch vorhandene ACLs, die auf den alten Benutzernamen verweisen, erteilt. Veraltete UUIDs in ACLs (aufgrund gelöschter Benutzer und Gruppen) werden vom Policy Director Management Server (**pdmgrd**) entfernt.

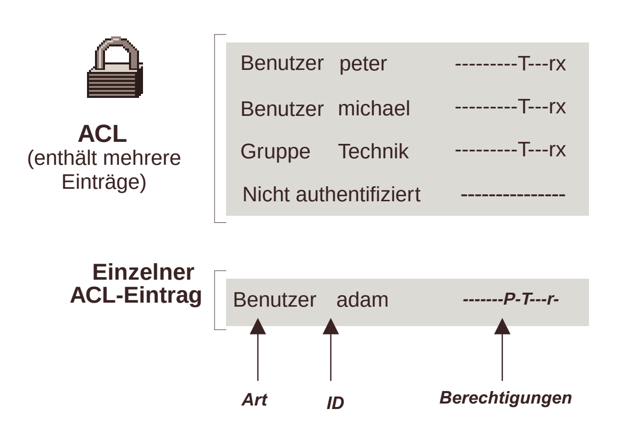



*Abbildung 17. Zugriffssteuerungsliste für ein Webseitenobjekt*

Sie verwenden das Dienstprogramm **pdadmin** oder den Web Portal Manager zum Erstellen, Ändern und Löschen von ACL-Einträgen.

## ACL-Policies erstellen und benennen

Sie können mit Hilfe des Web Portal Manager oder mit Hilfe des Befehls **pdadmin acl create** eine eindeutige ACL-Policy erstellen und mit einem Namen sichern. Dann können Sie eine Sicherheits-Policy anwenden, indem die ACL Objekten im geschützten Objektbereich zugeordnet wird.

Die Zugriffssteuerungsliste (ACL) wird zu einer ausschließlichen Policy (wie eine Formel oder ein Rezept) mit den spezifischen Einträgen, die die richtige Sicherungsstufe für alle ihr zugeordneten Objekte zur Verfügung stellen. Wenn sich die Anforderungen der Sicherheits-Policy ändern, editieren Sie nur die einzelne ACL. Die neue Sicherheitsdefinition wird sofort für alle Objekte, die dieser ACL zugeordnet sind, implementiert.

# Syntax der ACL-Einträge

Ein ACL-Eintrag enthält entweder zwei oder drei Attribute, je nach ACL-Eintragsart, und hat folgendes Format:

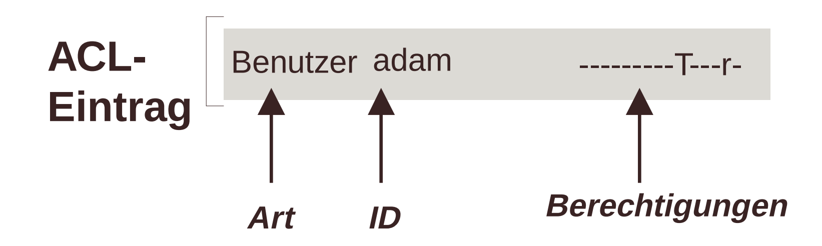



*Abbildung 18. Attribute für ACL-Einträge*

- **Art** – Die Definitionseinheitenkategorie (Benutzer oder Gruppe), für die die ACL erstellt wurde
- **ID (Identität)** – die eindeutige Kennung (Name) der Definitionseinheit

  Das Attribut ID ist für die ACL-Eintragsarten **Beliebige andere** und **Nicht authentifiziert** nicht erforderlich
- **Berechtigungen (oder Aktionen)** – die Operationen, die dieser Benutzer bzw. diese Gruppe für das Objekt ausführen kann

Die meisten Berechtigungen legen fest, ob ein Client eine spezifische Operation auf der Ressource ausführen kann.

In dem Beispiel oben hat der Benutzer **adam** (Art = Benutzer, ID = adam) die Berechtigung, das Objekt, das durch diese ACL-Policy geschützt wird, zu lesen (anzuzeigen). Die Berechtigung “r” gestattet Leseoperationen.Die Berechtigung “T” erzwingt die Traverse-Regel.

## Attribut ’Art’

Ein ACL-Eintrag **Art** gibt den Benutzer, die Gruppe oder die spezielle Definitionseinheit für einen bestimmten ACL-Eintrag an. Es gibt vier ACL-Eintragsarten:

| Art | Beschreibung |
|---|---|
| **Benutzer** | Definiert Berechtigungen für einen bestimmten Benutzer in der gesicherten Domäne. Der Benutzer muss ein Mitglied der gesicherten Domäne mit einem Konto in der Registrierungsdatenbank sein. Die Eintragsart ’Benutzer’ erfordert einen Benutzernamen (ID). Das Eintragsformat ist: `Benutzer-ID Berechtigungen`<br><br>Zum Beispiel:<br>`Benutzer Anthony -------T-----r-` |
| **Gruppe** | Definiert Berechtigungen für alle Mitglieder einer bestimmten Gruppe in der gesicherten Domäne. Die Eintragsart ’Gruppe’ erfordert einen Gruppennamen (ID). Das Eintragsformat ist: `Gruppen-ID Berechtigungen`<br><br>Zum Beispiel:<br>`Gruppe Technik -------T-----r-` |
| **Beliebige andere** (auch ’Beliebige authentifizierte’) | Definiert Berechtigungen für alle authentifizierten Benutzer. Es ist keine ID-Angabe erforderlich. Das Eintragsformat ist: `Beliebige andere Berechtigungen`<br><br>Zum Beispiel:<br>`Beliebige andere -------T-----r-` |

| Art | Beschreibung |
| --- | --- |
| **Nicht authentifiziert** | Definiert Berechtigungen für die Benutzer, die nicht durch den Sicherheitsserver authentifiziert wurden. Es ist keine ID-Angabe erforderlich. Das Eintragsformat ist: `Nicht authentifiziert Berechtigungen`<br><br>Zum Beispiel:<br>`Nicht authentifiziert -------T-----r-`<br><br>Dieser ACL-Eintrag ist eine Maske (eine bitweise “UND”-Operation) für den ACL-Eintrag **Beliebige andere**, mit der die definierte Berechtigung festgestellt wird. Für **Nicht authentifiziert** wird nur dann eine Berechtigung erteilt, wenn die Berechtigung auch im Eintrag **Beliebige andere** erscheint. Beispiel: Der folgende ACL-Eintrag **Nicht authentifiziert**:<br>`Nicht authentifiziert -------------rw`<br><br>der mit dem folgenden ACL-Eintrag **Beliebige andere** verglichen wird:<br>`Beliebige andere -------T-----r-`<br><br>resultiert in den folgenden Berechtigungen:<br>`-------------r- (Lesezugriff).` |

## Attribut ID

Der ACL-Eintrag **ID** ist die eindeutige Kennung (Name) für die Eintragsart ’Benutzer’ oder ’Gruppe’. IDs müssen gültige Benutzer und/oder Gruppen, die für die gesicherte Domäne erstellt und in der Registrierungsdatenbank gespeichert werden, angeben.

Beispiele:

```
Benutzer Michael

Benutzer Anthony

Gruppe Technik

Gruppe Dokumentation

Gruppe Fakturierung
```

**Anmerkung:** Das Attribut ID wird für die ACL-Eintragsarten **Beliebige andere** und **Nicht authentifiziert** nicht verwendet.

## Attribut Berechtigungen (Aktionen)

Jeder ACL-Eintrag enthält eine Reihe von **Berechtigungen** (oder Aktionen), die die Operationen beschreiben, die der Benutzer oder die Gruppe für das Objekt ausführen können.

ACL-Policies steuern geschützte Ressourcen wie folgt:

- Die Möglichkeit eines Benutzers, Operationen für geschützte Objekte auszuführen
- Die Möglichkeit eines Administrators, die Zugriffssteuerungsregeln für das Objekt und alle untergeordneten Objekte zu ändern
- Die Möglichkeit von Policy Director, Benutzerberechtigungen zu delegieren

**Anmerkung:** ACL-Berechtigungen sind kontextabhängig — die Funktionsweise bestimmter Berechtigungen variiert gemäß dem geschützten Objektbereich, in dem sie angewendet werden. Die Berechtigung **m** hat beispielsweise bei einem WebSEAL-Objekt eine andere Bedeutung als bei einem Management-Objekt.

## Policy Director-Standardberechtigungen (Aktionen)

Policy Director definiert 17 Standardberechtigungen (Aktionen). Web Portal Manager unterteilt diese Berechtigungen in drei Kategorien:

| **Basis** | **Generisch** | **WebSEAL** |
|---|---|---|
| `a A b B c g N t T W` | `d m s v` | `l r x` |

| Aktionsbit | Beschreibung | Kategorie |
|---|---|---|
| **a** | Attach | Basis |
| **A** | Add | Basis |
| **b** | Browse | Basis |
| **B** | Bypass TOD | Basis |
| **c** | Control | Basis |
| **d** | Delete | Generisch |
| **g** | Delegation | Basis |
| **l** | List Directory | WebSEAL |
| **m** | Modify | Generisch |
| **N** | Create | Basis |
| **r** | Read | WebSEAL |
| **s** | Server Administration | Generisch |
| **t** | Trace | Basis |
| **T** | Traverse | Basis |
| **v** | View | Generisch |
| **W** | Password | Basis |
| **x** | Execute | WebSEAL |

Policy Director ermöglicht die Definition zahlreicher zusätzlicher Berechtigungen (Aktionen) für die Verwendung durch Anwendungen eines anderen Herstellers. Siehe „Erweiterte ACL-Aktionen und Aktionsgruppen erstellen” auf Seite 81.

## Wie der Berechtigungsservice ACL-Policies verwendet

Policy Director gibt mit Hilfe von ACL-Policies die Bedingungen an, die für die Ausführung einer Operation mit einem geschützten Objekt erforderlich sind.

Wenn einem Objekt eine ACL-Policy zugeordnet wird, geben die Einträge in der ACL-Policy an, welche Operationen für dieses Objekt zulässig sind und wer diese Operationen ausführen darf.

Policy Director verwendet eine Standardberechtigungsgruppe, die einen breiten Operationsbereich abdeckt. Berechtigungen werden durch einzelne, druckbare ASCII-Zeichen (a-z, A-Z) dargestellt. Jede Berechtigung wird (durch **pdadmin** oder Web Portal Manager) mit einer Bezeichnung, die die betreffende Operation beschreibt, angezeigt. Außerdem gruppiert Web Portal Manager die ACL-Policies nach ihrer Verwendung in einem bestimmten Abschnitt des Objektbereichs (z. B. WebSEAL) oder nach ihrer Verwendung im gesamten Objektbereich (Basis, Generisch).

### Operationen für ein Objekt ausführen

Anwendungssoftware enthält normalerweise mindestens eine Operation, die für geschützte Objekte ausgeführt wird. Policy Director macht es erforderlich, dass diese Anwendungen den Berechtigungsservice aufrufen müssen, bevor die angeforderte Operation fortgesetzt werden darf. Dieser Aufruf erfolgt über die Berechtigungs-API sowohl für Policy Director-Services (z. B. WebSEAL) als auch für Anwendungen anderer Hersteller.

Der Berechtigungsservice trifft mit Hilfe der Informationen in der ACL-Policy eine einfache Entscheidung “Ja” oder “Nein” für die Frage: “Verfügt dieser Benutzer (diese Gruppe) über die Berechtigung ‘r’ (zum Beispiel) zum ‘Anzeigen’ des angeforderten Objekts?”

Der Berechtigungsservice weiß hierbei nichts von der Operation, für die die Berechtigung “r” benötigt wird. Für den Berechtigungsservice

ist nur die Tatsache von Bedeutung, ob die Berechtigung “r” im ACL-Eintrag des anfordernden Benutzers oder der anfordernden Gruppe vorhanden ist oder nicht.

Dies ist eine sehr wirksame Funktion des Berechtigungsservice. Der Service ist vollkommen unabhängig von den angeforderten Operationen. Aus diesem Grund ist es einfach, die Vorteile des Berechtigungsservice auf Anwendungen anderer Hersteller auszuweiten.

## Voraussetzungen für angepasste Berechtigungen

Das gesamte Repertoire der 18 Policy Director-Standardberechtigungen (Aktionen) steht Anwendungen anderer Hersteller zur Verfügung. Wenn eine Anwendung eines anderen Herstellers eine der Policy Director-Standardberechtigungen nutzt, sollte die zugeordnete Operation sehr genau der Operation entsprechen, die normalerweise von Policy Director ausgeführt wird. Die Berechtigung “r” sollte beispielsweise nur von einer Operation verwendet werden, bei der Lesezugriff für ein geschütztes Objekt benötigt wird.

**Anmerkung:** Eine Anwendung eines anderen Herstellers kann selbstverständlich eine Policy Director-Standardberechtigung für eine vollkommen andere Operation verwenden, weil der Berechtigungsservice keine Rücksicht auf die Operation nimmt. Diese Situation würde jedoch einem Administrator Schwierigkeiten bereiten, der dann zwischen zwei unterschiedlichen Verwendungen derselben Berechtigung unterscheiden müsste.

Bei einer Operation einer Anwendung eines anderen Herstellers, die durch keine der Standardberechtigungen richtig dargestellt wird, gestattet Policy Director die Definition einer neuen Berechtigung (Aktion), die diese Anwendung verwenden kann und vom Berechtigungsservice erkannt wird.

Siehe „Erweiterte ACL-Aktionen und Aktionsgruppen erstellen” auf Seite 81.

## Beispiel für angepasste Berechtigung

In diesem Beispiel muss eine Druckereinheit vor unberechtigter Verwendung geschützt werden. Ein Spool-Service für Drucker eines anderen Herstellers wird mit der Berechtigungs-API erstellt, so dass er den Berechtigungsservice für die Ausführung von ACL-Prüfungen für Anforderungen an den Drucker aufrufen kann.

Zu den Policy Director-Standardberechtigungen gehört keine eindeutige Berechtigung für den Schutz von Druckern. Der Drucker kann jedoch durch eine neu erstellte Berechtigung ("p" in diesem Beispiel) geschützt werden.

Dem Druckerobjekt wird eine ACL-Policy zugeordnet. Wenn ein Benutzer die Verwendung des geschützten Druckers anfordert, muss er über einen ACL-Eintrag verfügen, der die Berechtigung "p" enthält. Der Berechtigungsservice gibt eine positive Antwort aus, wenn die Berechtigung "p" vorhanden ist, und die Druckoperation wird fortgesetzt. Findet der Berechtigungsservice keine Berechtigung "p" für den betreffenden Benutzer, kann die Druckoperation nicht fortgesetzt werden.

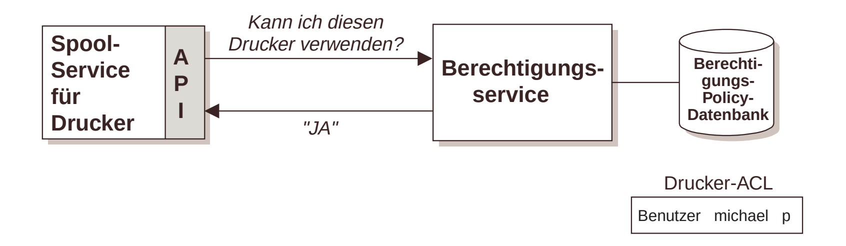



*Abbildung 19. Angepasste Berechtigung für Druck-Spooler*

# Zugriffssteuerungsliste (ACL) auswerten

Policy Director bestimmt die Berechtigungen, die einem bestimmten Benutzer durch eine Zugriffssteuerungsliste (ACL) erteilt wurden, mit Hilfe eines spezifischen Prüfprozesses. Wenn Sie diesen Prozess verstehen, können Sie bestimmen, wie Sie den unerwünschten Zugriff bestimmter Benutzer auf Ressourcen verhindern können.

## Authentifizierte Anforderungen auswerten

Policy Director prüft die Anforderung eines authentifizierten Benutzers in der folgenden Reihenfolge:

1. Vergleich der Benutzer-ID mit den Benutzereinträgen der Zugriffssteuerungsliste. Die erteilten Berechtigungen sind in dem übereinstimmenden Eintrag.

   *Übereinstimmung: Die Prüfung stoppt hier. Keine Übereinstimmung: Weiter mit dem nächsten Schritt.*

2. Bestimmung der Gruppe(n), zu der (denen) der Benutzer gehört und Vergleich mit den Gruppeneinträgen der Zugriffssteuerungsliste:

   Stimmen mehrere Gruppeneinträge überein, sind die resultierenden Berechtigungen eine logische “Oder-Verknüpfung” (geringste Einschränkung) der Berechtigungen, die durch jeden übereinstimmenden Eintrag erteilt werden.

   *Übereinstimmung: Die Prüfung stoppt hier. Keine Übereinstimmung: Weiter mit dem nächsten Schritt.*

3. Erteilen der Berechtigungen des Eintrags **Beliebige andere** (falls vorhanden).

   *Übereinstimmung: Die Prüfung stoppt hier. Keine Übereinstimmung: Weiter mit dem nächsten Schritt.*

4. Eine implizite Definitionseinheit ″Beliebige andere″ ist vorhanden, wenn kein ACL-Eintrag **Beliebige andere** vorhanden ist. Dieser implizite Eintrag erteilt keine Berechtigungen.

   *Übereinstimmung: Keine Berechtigungen erteilt. Ende des Prüfprozesses.*

## Nicht authentifizierte Anforderungen auswerten

Policy Director prüft einen nicht authentifizierten Benutzer durch Erteilen der Berechtigungen aus dem ACL-Eintrag **Nicht authentifiziert**.

Der Eintrag **Nicht authentifiziert** ist eine Maske (eine bitweise “UND”-Operation) für den Eintrag **Beliebige andere**, wenn Berechtigungen bestimmt werden. Für **Nicht authentifiziert** wird nur dann eine Berechtigung erteilt, wenn die Berechtigung auch im Eintrag **Beliebige andere** erscheint.

Da **Nicht authentifiziert** von **Beliebige andere** abhängig ist, hat es wenig Sinn, wenn eine Zugriffssteuerungsliste **Nicht authentifiziert** ohne **Beliebige andere** enthält. Wenn eine Zugriffssteuerungsliste **Nicht authentifiziert** ohne **Beliebige andere** enthält, lautet die Standardantwort, keine Berechtigungen für **Nicht authentifiziert** zu erteilen.

## Beispiel-ACL-Einträge

Berechtigungen für bestimmte Benutzer und Gruppe definieren Sie durch Angabe der entsprechenden ACL-Eintragsart. Im folgenden Beispiel hat die Gruppe **Dokumentation** uneingeschränkte Zugriffsberechtigungen:

```
Gruppe Dokumentation --bcg--Tdmsv--lrx
```

Sie können den Zugriff für andere authentifizierte Benutzer in der gesicherten Domäne, die nicht zur Gruppe ″Dokumentation″ gehören, durch Angabe der Eintragsart **Beliebige andere** einschränken:

```
Beliebige andere -------T-------rx
```

Den Zugriff auf die Eintragsart **Nicht authentifiziert** können Sie für Benutzer, die nicht zur gesicherten Domäne gehören, weiter einschränken.

```
Nicht authentifiziert -------T-------r-
```

**Anmerkung:** Ohne einen ACL-Eintrag **Nicht authentifiziert** können nicht authentifizierte Benutzer auf keine gesicherten Dokumente in der gesicherten Domäne zugreifen.

# Schlankes ACL-Modell: ACL-Übernahme

Damit Netzressourcen in einem geschützten Objektbereich gesichert werden, muss jedes Objekt durch eine ACL-Policy (ACL = Access Control List, Zugriffssteuerungsliste) geschützt werden.

Sie können einem Objekt eine ACL-Policy auf zwei Arten zuordnen:

- Dem Objekt eine **explizite** ACL-Policy zuordnen.
- Dem Objekt das **Übernehmen** seiner ACL-Policy von einem vorhergehenden Containerobjekt in der Hierarchie ermöglichen.

Das Übernehmen eines ACL-Schemas kann die Verwaltungs-Tasks für eine gesicherte Domäne beträchtlich reduzieren. In diesem Abschnitt wird der Begriff der übernommenen oder schlanken ACL-Policies erläutert.

## Erläuterungen zum schlanken ACL-Modell

Die Übernahme einer ACL-Policy beruht auf dem folgenden Prinzip: Jedes Objekt ohne explizit zugeordnete ACL-Policy übernimmt die Policy seines nächsten Containerobjekts mit einer explizit definierten ACL-Policy. Das heißt, alle Objekte *ohne* explizit zugeordnete ACL-Policies übernehmen ACL-Policies von Containerobjekten *mit* explizit zugeordneten ACL-Policies. Eine Übernahmekette wird unterbrochen, wenn Sie einem Objekt eine explizite ACL-Policy zuordnen.

ACL-Übernahme vereinfacht das Definieren und Verwalten von Zugriffssteuerungen für einen großen geschützten Objektbereich. In einem typischen Objektbereich müssen Sie nur ein paar ACL-Policies an Schlüsselpositionen zuordnen, um den gesamten Objektbereich zu sichern — daher der Begriff **schlankes** ACL-Modell.

Ein typischer Objektbereich beginnt mit einer einzelnen expliziten ACL, die dem **Stamm**containerobjekt (Root) zugeordnet wird. Die **Stamm**-ACL muss immer vorhanden sein und kann nie entfernt werden. Normalerweise ist dies eine ACL mit sehr wenig Einschränkungen. Alle Objekte in dem untergeordneten Objektbereich übernehmen diese ACL.

Wenn ein Bereich oder eine untergeordnete Baumstruktur in dem Objektbereich andere Zugriffssteuerungseinschränkungen erfordert, ordnen Sie eine explizite ACL am Stamm (Root) dieser untergeordneten Baumstruktur zu. Dadurch wird die Kette der übernommenen ACLs vom primären **Stamm**objektbereich zu dieser untergeordneten Baumstruktur unterbrochen. An dieser neu erstellten expliziten ACL beginnt eine neue Übernahmekette.

## Die Standardstamm-ACL-Policy

Policy Director startet die Überprüfung der Übernahme am **Stamm** (Root) des geschützten Objektbereichs. Wenn Sie für andere Objekte in der Baumstruktur ACLs nicht explizit definieren, übernimmt die gesamte Baumstruktur diese **Stamm**-ACL.

Am **Stamm** (Root) des geschützten Objektbereichs ist immer eine explizite ACL-Policy definiert. Ein Administrator kann diese ACL-

Policy durch eine andere mit anderen Einträgen und Berechtigungseinstellungen ersetzen. Die **Root**-ACL-Policy kann jedoch nie vollständig entfernt werden.

Die **Stamm**-ACL-Policy wird während der Policy Director-Erstinstallation und -konfiguration explizit definiert.

Zu den Kerneinträgen der Standardstamm-ACL, **default-root**, gehören:

```
Gruppe iv-admin              Tcmdbva
Beliebige andere            T
Nicht authentifiziert       T
```

## Berechtigung Traverse

Die Zugriffssteuerung von Policy Director ist von zwei Bedingungen abhängig.

1. Die ACL (Zugriffssteuerungsliste), die das angeforderte Objekt steuert, muss entsprechende Zugriffsberechtigungen für den anfordernden Benutzer enthalten.
2. Der anfordernde Benutzer muss auf das angeforderte Objekt zugreifen können.

   Die Zugriffsmöglichkeit für geschützte Objekte wird durch die Berechtigung traverse (**T**) gesteuert.

Die Berechtigung traverse wird nur auf Containerobjekte im geschützten Objektbereich angewendet. Die Berechtigung traverse legt fest, dass ein Benutzer, eine Gruppe, Beliebige andere oder Nicht authentifizierte, die im ACL-Eintrag angegeben sind, die Berechtigung haben, dieses Objekt zu durchqueren, um Zugriff auf ein geschütztes Ressourcenobjekt, das sich an einer untergeordneten Position in der Hierarchie befindet, zu erhalten.

Ein Requester kann auf ein geschütztes Objekt zugreifen, wenn er in jeder ACL, die Containerobjekten über der angeforderten Ressource in dem Pfad zum Stamm (einschließlich) zugeordnet ist, über die Berechtigung traverse verfügt.

Das folgende Beispiel zeigt, wie die Berechtigung traverse funktioniert. In der ACME Corporation gibt es ein Containerobjekt (Verzeichnis) `Technik`, das ein Containerobjekt (Unterverzeichnis) `TechPubs` enthält. **Benutzer kate**, ein Mitglied der Abteilung 'Verkauf', benötigt die Berechtigung traverse für das Verzeichnis `Technik/TechPubs`, um eine Release-Informationsdatei zu überprüfen. Der Administrator stellt die Berechtigung traverse für **Beliebige andere** am Stamm (Root) zur Verfügung. Der Administrator stellt die Berechtigung traverse für **Gruppe Verkauf** im Verzeichnis `Technik` zur Verfügung. Das Verzeichnis `TechPubs` übernimmt die ACL aus dem Verzeichnis `Technik`. Auch wenn Kate keine anderen Berechtigungen in diesen beiden Verzeichnissen hat, kann sie diese Verzeichnisse durchqueren (traverse), um auf die Datei `release_note` zuzugreifen. Da diese Datei über Lesezugriffsberechtigung für **Benutzer Kate** verfügt, kann Kate die Datei anzeigen.

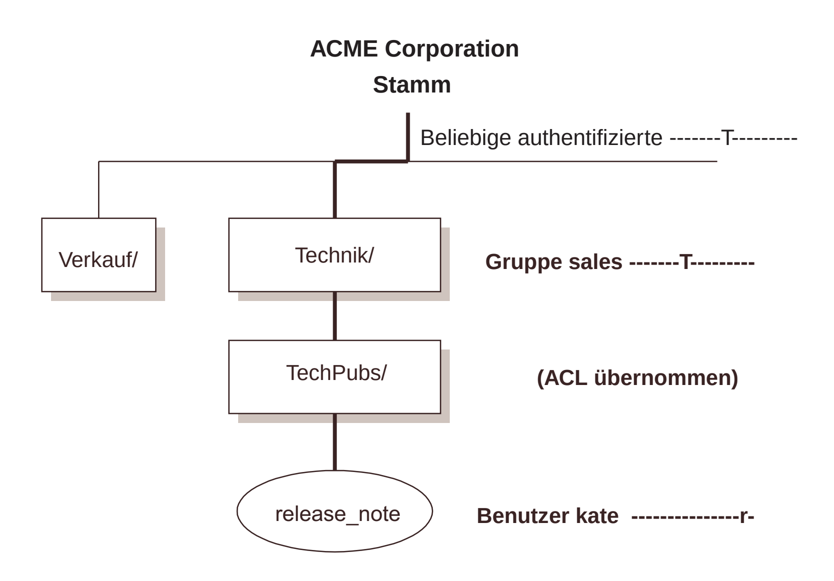



*Abbildung 20. Berechtigung traverse*

Sie können den Zugriff auf die Hierarchie unterhalb eines bestimmten Containerobjekts leicht einschränken — ohne einzelne Berechtigungen für diese Objekte neu zu definieren.

Sie entfernen einfach die Berechtigung traverse aus dem entsprechenden ACL-Eintrag. Das Entfernen der Berechtigung traverse bei einem Verzeichnisobjekt schützt alle Objekte, die sich an einer untergeordneten Position in der Hierarchie befinden, auch wenn diese Objekte andere, weniger restriktive ACLs enthalten.

Wenn **Gruppe Verkauf** beispielsweise nicht über die Berechtigung traverse für das Verzeichnis `Technik` verfügt, kann Kate nicht auf die Releasebeschreibungsdatei zugreifen, auch wenn sie über Lesezugriff für die Datei verfügt.

## Zugriffsanforderungen auflösen

Die Übernahme beginnt mit der **Stamm-**ACL-Policy und betrifft alle Objekte in dem Objektbereich, bis ein Objekt mit einer expliziten ACL-Policy erreicht wird. An diesem Punkt beginnt eine neue Übernahmekette.

Objekte unter einer explizit definierten ACL-Policy übernehmen die neuen Zugriffssteuerungseinstellungen. Wenn Sie eine explizite ACL-Policy löschen, kehrt die Zugriffssteuerung zum nächsten Verzeichnis oder Containerobjekt mit einer explizit definierten ACL-Policy zurück.

Wenn ein Benutzer versucht, auf ein gesichertes Objekt (z. B. ein Webdokument) zuzugreifen, überprüft Policy Director, ob der Benutzer über die Berechtigungen für den Zugriff auf das Objekt verfügt. Dies erfolgt durch Überprüfen jedes Objekts entlang der Objekthierarchie auf die richtigen übernommenen oder explizit definierten Berechtigungen.

Einem Benutzer wird der Zugriff auf ein Objekt verweigert, wenn ein Verzeichnis oder Containerobjekt in der übergeordneten Hierarchie nicht die Berechtigung traverse für diesen Benutzer enthält. Der Zugriff wird außerdem verweigert, wenn das Zielobjekt keine ausreichenden Berechtigungen zum Ausführen der angeforderten Operation enthält.

Ein anfordernder Benutzer muss über *beide* folgende Berechtigungen verfügen, um eine Zugriffsprüfung zu bestehen:

1. Berechtigung zum Durchlaufen (Traverse) des Pfads zum angeforderten Objekt.
2. Geeignete Berechtigungen für das angeforderte Objekt.

Das folgende Beispiel zeigt den Prozess, bei dem geprüft wird, ob ein Benutzer ein Objekt lesen (anzeigen) kann:

```
/acme/engineering/project_Y/current/report.html
```

Policy Director prüft:

1. Berechtigung traverse in der explizit definierten **Stamm**-ACL-Policy (/).
2. Berechtigung traverse in allen expliziten ACL-Policies, die den folgenden Verzeichnissen zugeordnet sind: `acme`, `engineering`, `project_Y` und `current`.
3. Lesezugriff für die Datei selbst (`report.html` ).

Dem Benutzer wird der Zugriff verweigert, wenn er die Zugriffsprüfung an einem dieser Punkte in der Objekthierarchie nicht besteht.

## ACL-Policies für verschiedene Objektarten anwenden

In einer ACL-Policy können Berechtigungen für eine ganze Reihe von Operationen definiert werden. Für ein bestimmtes Objekt, dem die ACL-Policy zugeordnet ist, ist aber möglicherweise nur ein Teil dieser möglichen Operationen relevant.

Der Grund hierfür steht im Zusammenhang mit den beiden Policy Director-Funktionen, die die Verwaltung vereinfachen sollen:

- ACL-Policies
- ACL-Übernahme

Mit Hilfe von ACL-Policies können Sie eine ACL-Definition mehreren Objekten im geschützten Objektbereich zuordnen. Die ACL-Definition besteht aus so vielen Einträgen, dass die Anforderungen aller

Objekte, für die die ACL-Policy angewendet wird, erfüllt werden. Für ein einzelnes Objekt können jedoch jeweils nur einige der Einträge von Bedeutung sein.

Im ACL-Übernahmemodell “übernimmt” jedes Objekt ohne explizite ACL-Policy die Policy-Definitionen der nächsten ACL-Policy, die für ein übergeordnetes Objekt in der Hierarchie angewendet wird.

Zusammenfassung: Eine ACL-Policy muss die erforderlichen Berechtigungen für alle Objektarten, auf die sie angewendet wird, beschreiben (nicht nur für das Objekt, dem sie zugeordnet ist).

## Beispiel einer ACL-Policy-Übernahme

Die folgende Abbildung zeigt die Auswirkung einer Mischung aus übernommenen und expliziten ACL-Policies in einem Unternehmensobjektbereich.

In einem Unternehmensobjektbereich ist eine allgemeine Sicherheits-Policy am **Stamm**objekt (Root) definiert. Dem **Stamm** folgt das Containerobjekt `/WebSEAL` und einzeln gesteuerte, untergeordnete Baumstrukturen verschiedener Abteilungen.

In diesem Beispiel hat die Gruppe **Verkauf** das Eigentumsrecht ihrer untergeordneten Abteilungsbaumstruktur. Beachten Sie, dass die ACL-Policy in dieser untergeordneten Baumstruktur die Eintragsarten **Nicht authentifiziert** und **Beliebige andere** nicht mehr berücksichtigt.

Die Datei mit dem Umsatz bis dato (`ytd.html`) verfügt über eine explizite ACL-Policy, die Lesezugriff für Mitglieder der Gruppe **Verkauf-vp** erteilt (die auch zur Gruppe **Verkauf** gehören).

**Anmerkung:** Dieses ACL-Schema muss beim Hinzufügen oder Entfernen von Benutzern innerhalb der gesicherten Domäne nicht geändert werden. Neue Benutzer werden einfach der (den) entsprechenden Gruppe(n) hinzugefügt. Genauso können Benutzer aus diesen Gruppen entfernt werden.

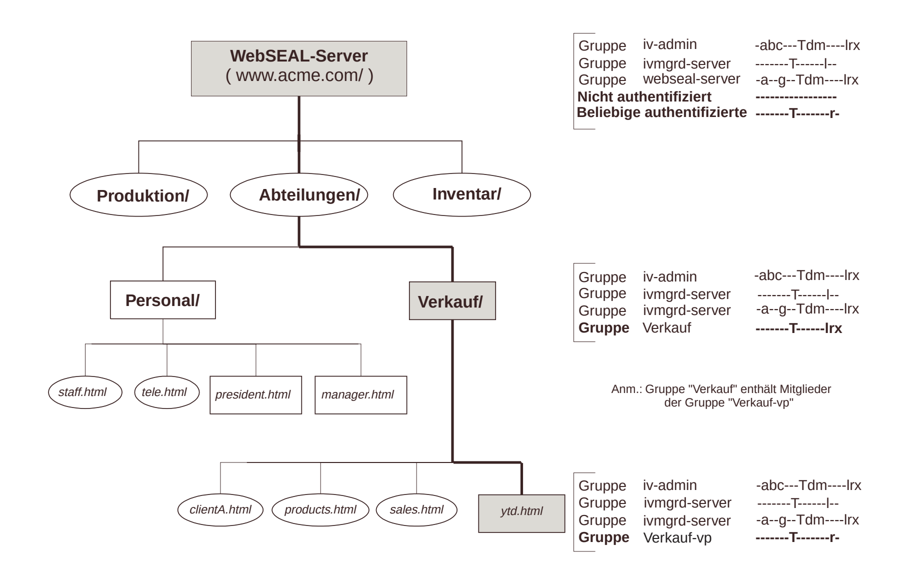



*Abbildung 21. ACL-Übernahmebeispiel*

# Richtlinien für einen geschützten Objektbereich

- Definieren Sie eine Sicherheits-Policy auf hoher Ebene für Containerobjekte am Anfang des Objektbereichs. Definieren Sie mit Hilfe von expliziten ACL-Policies für untergeordnete Objekte in der Hierarchie Ausnahmen dieser Policy.
- Ordnen Sie Ihren geschützten Objektbereich so, dass die meisten Objekte durch übernommene und nicht durch explizite ACL-Policies geschützt werden.

  Übernommene ACL-Policies vereinfachen die Verwaltung Ihrer Baumstruktur, weil hierdurch die Anzahl der zu verwaltenden ACL-Policies reduziert wird. Dadurch verringert sich auch das Risiko eines Fehlers, der Ihr Netz gefährden könnte.
- Platzieren Sie neue Objekte in der Baumstruktur an Positionen, an denen sie die entsprechenden Berechtigungen übernehmen können.

Teilen Sie Ihre Objektbaumstruktur in untergeordnete Baumstrukturen auf, wobei jede untergeordnete Baumstruktur durch eine bestimmte Zugriffs-Policy gesteuert wird. Die Zugriffs-Policy für eine vollständige untergeordnete Baumstruktur legen Sie fest, indem Sie eine explizite ACL-Policy am Stamm (Root) der untergeordneten Baumstruktur definieren.

- Erstellen Sie eine Reihe von ACL-Kern-Policies, und verwenden Sie diese ACL-Policies wo immer erforderlich.

  Da eine ACL-Policy eine Zentraldefinition ist, wirken sich alle Änderungen der Policy auf alle Objekte, die dieser ACL-Policy zugeordnet sind, aus.

- Steuern Sie den Benutzerzugriff mit Hilfe von Gruppen.

  Eine ACL-Policy kann ausschließlich aus Gruppeneinträgen bestehen. Der Zugriff auf ein Objekt durch einzelne Benutzer kann durch Hinzufügen und Entfernen von Benutzern in diesen Gruppen gesteuert werden.

## Erweiterte ACL-Aktionen und Aktionsgruppen erstellen

In diesem Abschnitt hat das Wort “Aktion” dieselbe Bedeutung wie das Wort “Berechtigung”, das in vorangegangenen Abschnitten verwendet wurde.

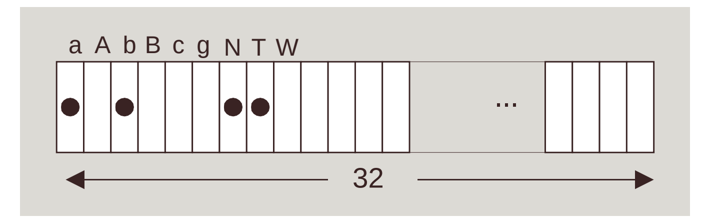
Jede Policy Director-Berechtigung wird als eine Aktion definiert. Siebzehn Aktionen sind für unmittelbare Funktionalität vordefiniert (siehe „Policy Director-Standardberechtigungen (Aktionen)” auf Seite 67). Sie können auch neue Aktionen für Anwendungen anderer Hersteller definieren.

Dieser Abschnitt beschreibt, wie Sie Aktionsgruppen definieren, die als Container für eine erweiterte Gruppe angepasster Aktionen dienen:

- In jeder Aktionsgruppe können sich bis zu 32 Aktionsbits befinden.
- Ein Aktionsbit besteht aus einem Buchstaben von a-z oder A-Z.

- Jedes Aktionsbitzeichen kann nur einmal in einer Aktionsgruppe verwendet werden.
- Sie können ein Aktionsbit in verschiedenen Aktionsgruppen mehrfach verwenden.
- Die Policy Director-Standardaktionen sind in einer vordefinierten Aktionsgruppe mit dem Namen “primary” gespeichert.

**Primäre Aktionsgruppe**




Bits gesetzt für:
Gruppe sales abNT

*Abbildung 22. Aktionsgruppe ’primary’*

Policy Director unterstützt maximal 32 Aktionsgruppen (einschließlich der Aktionsgruppe ’primary’) für maximal 1024 Einzelaktionen.

**Mehrere Aktionsgruppen**

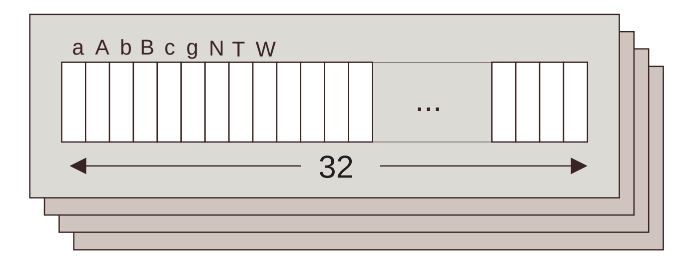



*Abbildung 23. Mehrere Aktionsgruppen*

## Neue Aktionsgruppe erstellen

Mit dem Befehl **pdadmin action group create** können Sie eine neue Aktionsgruppe erstellen:

```
pdadmin> action group create test-group
pdadmin> action group list
      primary
      test-group
pdadmin> action group delete test-group
pdadmin> action group list
      primary
```

Die Standardaktionsgruppe ’primary’ wird immer in einer Gruppenliste angezeigt und kann nicht gelöscht werden.

Sie müssen über einen Eintrag in einer Zugriffssteuerungsliste (ACL) im Objekt /Management/ACL mit der Berechtigung zum Ändern (m) verfügen, um Aktionsgruppen zu erstellen, und mit der Berechtigung zum Löschen (d), um Aktionsgruppen zu löschen.

## Neue Aktionen in einer Aktionsgruppe erstellen

Mit dem Befehl **pdadmin action create** können Sie eine neue Aktion in einer Aktionsgruppe erstellen:

```
pdadmin> action create <Aktionsname> <Aktionsbezeichnung> <Aktionsart>
<Aktionsgruppenname>
```

| **Aktionsname** | Die Aktion (Berechtigung) darstellender Buchstabe. |
|---|---|
| **Aktionsbezeichnung** | Beschreibung für diese Aktion. Wird in einem Befehl **pdadmin action list** und im Web Portal Manager angezeigt. |
| **Aktionsart** | Aktionskategorie (verwendet Web Portal Manager zum Zusammenfassen allgemeiner Aktionsbits). Die Standardkategorien sind Basis, Generisch und WebSEAL. |
| **Aktionsgruppenname** | Die Aktionsgruppe, zu der diese neue Aktion gehört. Wird dieses Argument nicht angegeben, wird die Aktion der Aktionsgruppe “primary” zugeordnet. |

Zum Beispiel:

```
pdadmin> action create P Test-Action Special test-group
pdadmin> action list test-group
      P  Test-Action  Special
pdadmin> action delete P test-group
pdadmin> action list test-group
pdadmin>
```

## Angepasste Aktionen in ACL-Einträge eingeben

Wie im Abschnitt „Syntax der ACL-Einträge” auf Seite 63 beschrieben, enthalten ACL-Einträge eine Eintragsart, eine Art-ID (für Benutzer- und Gruppenarten) und die Gruppe der zulässigen Aktionsbits.

Sie müssen für angepasste Aktionsbits, die nicht zur Aktionsgruppe “primary” gehören, eine spezielle Syntax verwenden. Aktionszeichenfolgen, die die Aktionsbits aus mehreren Aktionsgruppen darstellen, werden im folgenden Format angegeben:

```
<Aktion>...<Aktion>[<Aktionsgruppe>]<Aktion>...<Aktion>,,,
```

Zum Beispiel:

abgTr[groupA]Pq[groupB]Rsy[groupC]ab

- Die erste Aktionsbitgruppe (abgTr) stellt Berechtigungen aus der Aktionsgruppe “primary” (Policy Director-Standard) dar.
- Aktionsgruppe A enthält die Aktionen P und q.
- Aktionsgruppe B enthält die Aktionen R, s und y.
- Aktionsgruppe C enthält die Aktionen a und b.
- Beachten Sie, dass die Aktionsgruppe C Aktionsbits enthält, die dieselben Buchstaben wie Aktionsbits in der Gruppe “primary” verwenden.

  Da die Aktionsbits einer bestimmten Aktionsgruppe (C) zugeordnet sind, haben die Aktionsbits “a” und “b” eindeutige Identitäten und können ganz andere Berechtigungen als die Aktionsbits “a” und “b” in der Aktionsgruppe “primary” darstellen.

## Beispiel

### Aktionsgruppen anzeigen

```
pdadmin>
pdadmin> action group list
      primary
      test-group
```

### Aktionen in Aktionsgruppe “test-group” auflisten

```
pdadmin> action list test-group
      P  Test-Action  Special
      S  Test-Action2  Special
```

### ACL-Policies auflisten

```
pdadmin> acl list
      default-webseal
      default-root
      test
      default-replica
      default-management
```

### Details der Zugriffssteuerungsliste “test” anzeigen

```
pdadmin> acl show test
      ACL-Name: test
      Beschreibung:
      Einträge:
      Benutzer  sec_master  Tcmdbva
      Gruppe  ivmgrd-servers  Tl
      Beliebige andere  r
```

### ACL-Eintrag für Benutzer Kathy mit Aktionen aus den Aktionsgruppen “primary” und “test-group” hinzufügen

```
pdadmin> acl modify test set user kathy brT[test-group]PS
pdadmin> acl show test
      ACL-Name: test
      Beschreibung:
      Einträge:
      Benutzer  sec_master  Tcmdbva
      Gruppe  ivmgrd-servers  Tl
      Beliebige andere  r
      Benutzer  kathy  Tbr[test-group]PS
```

## ACL-Policies und der geschützte Objektbereich

Containerobjekte stellen bestimmte Bereiche des geschützten Objektbereichs dar und dienen zwei wichtigen Sicherheitsfunktionen:

1. Sie können mit Hilfe der Zugriffssteuerungsliste eines Containerobjekts Policy auf hoher Ebene für alle untergeordneten Objekte in dem Bereich definieren, wenn keine anderen expliziten Zugriffssteuerungslisten angewendet werden.
2. Sie können die Zugriffsberechtigung für alle Objekte in einem Bereich verweigern, indem Sie die Berechtigung zum Durchqueren traverse aus der Zugriffssteuerungsliste des Containerobjekts entfernen.

### Stammcontainerobjekt ( / )

Die folgenden Sicherheitshinweise betreffen das Stammobjekt (Root):

- Das **Stamm**objekt ist der Ausgangspunkt der ACL-Übernahmekette für den gesamten geschützten Objektbereich.
- Wenn Sie keine anderen expliziten ACLs anwenden, definiert das **Stamm**objekt (durch Übernahme) die Sicherheits-Policy für den gesamten Objektbereich.
- Für den Zugriff auf die Objekte, die sich unterhalb des **Stamm**objekts befinden, ist die Berechtigung traverse erforderlich.

### Berechtigung Traverse

Die Berechtigung traverse (Durchqueren) ist eine generische Berechtigung, die im gesamten geschützten Objektbereich gilt:

| | Operation | Beschreibung |
|---|---|---|
| **T** | Traverse | Erlaubt bei Anwendung auf ein Containerobjekt dem Requester, das Containerobjekt auf dem Weg zum angeforderten Ressourcenobjekt hierarchisch zu durchqueren. Es wird keine andere Art des Zugriffs für das Containerobjekt erteilt. Die Berechtigung traverse ist für das angeforderte Ressourcenobjekt selbst nicht erforderlich. |

## WebSEAL-Berechtigungen

Die folgenden Sicherheitshinweise betreffen den Container /WebSEAL im geschützten Objektbereich:

- Das Objekt WebSEAL ist der Ausgangspunkt der ACL-Übernahmekette für den Bereich WebSEAL im Objektbereich.
- Wenn Sie keine anderen expliziten ACLs anwenden, definiert dieses Objekt (durch Übernahme) die Sicherheits-Policy für den gesamten Webbereich.
- Für den Zugriff auf dieses Objekt und alle Objekte unterhalb dieses Punkts ist die Berechtigung traverse erforderlich.

### /WebSEAL/<*host*>

Diese untergeordnete Baumstruktur enthält den Webbereich eines bestimmten WebSEAL-Servers. Die folgenden Sicherheitshinweise betreffen dieses Objekt:

- Für den Zugriff auf alle Objekte unterhalb dieses Punkts ist die Berechtigung traverse erforderlich.
- Wenn Sie keine anderen expliziten ACLs anwenden, definiert dieses Objekt (durch Übernahme) die Sicherheits-Policy für den gesamten Objektbereich auf dieser Maschine.

### /WebSEAL/<*host*>/<*file*>

Dies ist das Ressourcenobjekt, das auf HTTP-Zugriff überprüft wird. Welche Berechtigungen überprüft werden, ist davon abhängig, welche Operation angefordert wird.

## WebSEAL-Berechtigungen

Die folgende Tabelle beschreibt die für den Bereich WebSEAL des Objektbereichs gültigen Berechtigungen:

| | Operation | Beschreibung |
|---|---|---|
| **r** | read | Das Webobjekt anzeigen. |
| **x** | execute | Das CGI-Programm ausführen. |
| **d** | delete | Das Webobjekt aus dem Webbereich entfernen. |
| **m** | modify | Eine PUT-Operation für ein HTTP-Objekt ausführen. (Ein HTTP-Objekt in den Objektbereich WebSEAL stellen - veröffentlichen.) |
| **l** | list | Benötigt der Verwaltungsserver zum Generieren einer automatischen Liste des Verzeichnisses des Webbereichs. |
| **g** | delegation | Ordnet einem WebSEAL-Server die Berechtigung zu, für einen Client zu agieren und diese Anforderung an einen über Junction verbundenen WebSEAL-Server zu übergeben. |

# Verwaltungsberechtigungen

Der Verwaltungsbereich (Management) des geschützten Objektbereichs enthält mehrere Verwaltungscontainersubobjekte, die bestimmte Berechtigungsgruppen erfordern:


- „/Management/ACL-Berechtigungen” auf Seite 90
- „/Management/Action-Berechtigungen” auf Seite 92
- „/Management/POP-Berechtigungen” auf Seite 93
- „/Management/Server-Berechtigungen” auf Seite 94
- „/Management/Config-Berechtigungen” auf Seite 94
- „/Management/Policy-Berechtigungen” auf Seite 95
- „/Management/Replica-Berechtigungen” auf Seite 95
- „/Management/Users-Berechtigungen” auf Seite 96
- „/Management/Groups-Berechtigungen” auf Seite 98
- „/Management/GSO-Berechtigungen” auf Seite 99


Die folgenden Sicherheitshinweise betreffen den Bereich /Management im geschützten Objektbereich:

- Das Verwaltungsobjekt (Management) ist der Ausgangspunkt der ACL-Übernahmekette für den gesamten Bereich /Management im Objektbereich.
- Wenn Sie keine anderen expliziten ACLs anwenden, definiert dieses Objekt (durch Übernahme) die Sicherheits-Policy für den gesamten Verwaltungsobjektbereich.
- Für den Zugriff auf /Management (Verwaltung) ist die Berechtigung traverse erforderlich.

## /Management/ACL-Berechtigungen

Mit diesem Objekt können Verwaltungsbenutzer ACL-Verwaltungs-Task auf hoher Ebene ausführen, die sich auf die Sicherheits-Policy für die gesicherte Domäne auswirken können.

| | Operation | Beschreibung |
|---|---|---|
| **a** | attach | ACL-Policies Objekten zuordnen; ACL-Policies aus Objekten entfernen.<br>`acl attach`<br>`acl detach` |
| **c** | control | Eigentumsrecht der ACL-Policy; erlaubt das Erstellen, Löschen und Ändern von Einträgen für diese ACL.<br>`acl modify` |
| **d** | delete | Vorhandene ACL-Policy löschen. Der ACL-Eintrag für diesen Benutzer muss außerdem die Berechtigung control (**c**) enthalten.<br>`acl delete` |
| **m** | modify | Neue ACL-Policy erstellen.<br>`acl create` |
| **v** | view | ACLs auflisten, suchen und anzeigen; ACL-Details anzeigen. Diese Berechtigung muss sich in einem Eintrag einer Zugriffssteuerungsliste befinden, die /Management/ACL zugeordnet ist.<br>`acl find`<br>`acl list`<br>`acl show` |

Sie müssen ACL-Administratoreinträge in der Standard-ACL-Policy für das Objekt /Management/ACL erstellen. Der ACL-Eintrag des Administrators kann alle der oben aufgeführten Berechtigungen enthalten. Diese Berechtigungen gestatten dem Administrator neue ACL-Policies zu erstellen, ACLs Objekten zuzuordnen und ACL-Policies zu löschen.

Ein ACL-Administrator kann eine vorhandene Zugriffssteuerungsliste (ACL) nur dann ändern, wenn diese Zugriffssteuerungsliste für den Administrator einen Eintrag enthält, der die Berechtigung control (**c**) enthält. Nur der Eigner einer Zugriffssteuerungsliste kann ihre Einträge ändern.

Beachten Sie, dass der Ersteller einer neuen ACL-Policy (**m** in /Management/ACL) der erste Eintrag in dieser Zugriffssteuerungsliste (ACL) wird — die Berechtigungen **TcmdbsvaBlNWA** sind hierbei standardmäßig definiert.

Wenn beispielsweise **sec_master** ein Administratoreintrag in der Zugriffssteuerungsliste **default-management** mit der Berechtigung **m** ist, kann **sec_master** eine neue ACL-Policy erstellen. Benutzer **sec_master** wird zum ersten Eintrag in der neuen ACL und verfügt über die Berechtigungen **TcmdbsvaBlNWA**.

Die Berechtigung control (**c**) verleiht **sec_master** das Eigentumsrecht für die Zugriffssteuerungsliste und gestattet **sec_master** das Ändern der Zugriffssteuerungsliste. Benutzer **sec_master** könnte dann anderen Benutzereinträgen in dieser Zugriffssteuerungsliste Verwaltungsberechtigungen erteilen.

Das Eigentumsrecht für die Zugriffssteuerungsliste **default-management** selbst wird sowohl dem Benutzer **sec_master** als auch der Gruppe **iv-admin** standardmäßig erteilt.

## Berechtigung Control (c)

Die Berechtigung control ist eine hohe Berechtigung, die Ihnen das Eigentumsrecht einer ACL-Policy verleiht. Mit Hilfe von control können Sie die Einträge in der ACL-Policy ändern. Das heißt, Sie haben die Berechtigung, Einträge zu erstellen und zu löschen und Berechtigungen zu erteilen und zu entziehen.

Der Administrator, der diese Zugriffssteuerungsliste (ACL) aus der Liste der ACL-Policies löschen will, muss über einen Eintrag in dieser ACL verfügen, und die Berechtigung control muss für den Administrator in diesem Eintrag definiert sein.

Die Berechtigung control gestattet, einem anderen Benutzer Verwaltungsberechtigungen zu erteilen, wie z. B. diese ACL Objekten zuzuordnen (Berechtigung attach **a**). Sie müssen die Berechtigung control aufgrund der starken Eigentumsrechteigenschaften mit großer Vorsicht verwenden.

Die Berechtigung control ist nur im Bereich /Management/ACL von Bedeutung.

## /Management/Action-Berechtigungen

Mit diesem Objekt können Verwaltungsbenutzer angepasste Aktionen und Aktionsgruppen verwalten. Aktions-Tasks und zugehörige Berechtigungen:

| | Operation | Beschreibung |
|---|---|---|
| **d** | delete | Vorhandene Aktion oder Aktionsgruppe löschen.<br>`action delete`<br>`action group delete` |
| **m** | modify | Neue Aktion oder Aktionsgruppe erstellen.<br>`action create`<br>`action group create` |
| | | `action list`<br>`action group list`<br><br>Erfordern keine speziellen Berechtigungen. |

Policy Director stellt Berechtigungsservices für Anwendungen zur Verfügung. Die zu der Policy Director-Produktfamilie gehörenden Anwendungen sind z. B. WebSEAL (für Webanwendungen) und PDMQ (für Nachrichtenanwendungen).

Anwendungen anderer Hersteller können Aufrufe an den Berechtigungsservice über die Berechtigungs-API durchführen.

Für die Integration einer Anwendung eines anderen Herstellers in den Berechtigungsservice sind zwei Schritte erforderlich:

- Den Objektbereich der Anwendung definieren
- Berechtigungen für Objekte (Ressourcen), die geschützt werden müssen, anwenden

Der Administrator eines Objektbereichs einer Anwendung eines anderen Herstellers kann mit Hilfe des Dienstprogramms **pdadmin** neue Berechtigungen und Aktionen definieren. Der Administrator muss über die Management/Action-Berechtigungen **m** und **d** zum Erstellen und Löschen dieser Berechtigungen/Aktionen verfügen.

## /Management/POP-Berechtigungen

Mit diesem Objekt können Verwaltungsbenutzer geschützte Objekt-Policies verwalten. Alle Berechtigungen müssen in Einträgen für Zugriffssteuerungslisten in /Management/POP erscheinen. Aktions-Tasks und zugehörige Berechtigungen:

| | Operation | Beschreibung |
|---|---|---|
| **a** | attach | Eine POP einem Objekt zuordnen.<br>`pop attach`<br>`pop detach` |
| **d** | delete | Eine POP löschen.<br>`pop delete` |
| **m** | modify | POPs erstellen und POP-Attribute ändern.<br>`pop create`<br>`pop modify` |
| **v** | view | POPs suchen und auflisten und POP-Details anzeigen.<br>`pop find`<br>`pop list`<br>`pop show` |
| **B** | Bypass TOD | Eine Verwaltungsberechtigung, die das POP-Attribut TOD (Time of Day, Uhrzeit) für ein Objekt überschreibt. |

## /Management/Server-Berechtigungen

Mit dem Containerobjekt **/Management/Server** des geschützten Objektbereichs können Administratoren Serververwaltungs-Tasks ausführen (wenn entsprechende Berechtigungen definiert sind).

Mit Hilfe von Steuerelementen für die Serververwaltung wird bestimmt, ob ein Benutzer über die Berechtigung zum Erstellen, Ändern oder Löschen einer Serverdefinition verfügt. Serverdefinitionen enthalten Informationen, mit denen andere Policy Director-Server, insbesondere der Management Server (**pdmgrd**), diesen Server lokalisieren und mit ihm Daten austauschen können.

Eine Serverdefinition wird während des Installationsprozesses für einen bestimmten Ressourcenmanager (z. B. WebSEAL) oder Authorization Server (**pdacld**) erstellt. Die Definition für einen Server wird außerdem gelöscht, wenn der Server deinstalliert wird.

| | Operation | Beschreibung |
|---|---|---|
| **s** | server | Berechtigungsdatenbank replizieren.<br>`server replicate` |
| **v** | view | Registrierte Server auflisten und Servereigenschaften anzeigen.<br>`server list`<br>`server show` |
| **t** | trace | Dynamischen Trace oder Statistikverwaltung aktivieren.<br>`server task <Servername> trace`<br>`server task <Servername> stats` |

## /Management/Config-Berechtigungen

Mit dem Containerobjekt **/Management/Config** des geschützten Objektbereichs können Administratoren Konfigurationsverwaltungs-Tasks ausführen (wenn entsprechende Berechtigungen definiert sind).

Erstellen und Löschen von Serverdefinitionen erfolgt automatisch — der Installationsadministrator muss keine besonderen Schritte für die Erstellung einer Definition ausführen. Dem Administrator muss jedoch die Berechtigung modify (**m**) für das Objekt

**/Management/Config** erteilt werden, damit die Definition während der Installation erstellt werden kann.

Außerdem muss der Administrator über die Berechtigung delete (**d**) für das Objekt **/Management/Config** verfügen, damit die Definition während der Deinstallation gelöscht werden kann.

| | Operation | Beschreibung |
|---|---|---|
| **m** | modify | Konfiguration in einer gesicherten Domäne.<br>`svrsslcfg -config`<br>`svrsslcfg -modify` |
| **d** | delete | Dekonfiguration.<br>`srvsslcfg -unconfig` |

## /Management/Policy-Berechtigungen

Mit dem Containerobjekt **/Management/Policy** des geschützten Objektbereichs können Administratoren die Befehl **policy get** und **policy set** berechtigen (wenn entsprechende Berechtigungen definiert sind).

| | Operation | Beschreibung |
|---|---|---|
| **v** | view | Erforderlich für **policy get**-Operationen. |
| **m** | modify | Erforderlich für **policy set**-Operationen. |

## /Management/Replica-Berechtigungen

Das Containerobjekt **/Management/Replica** des geschützten Objektbereichs steuert die Replikation (Vervielfältigung) der Berechtigungsdatenbank. Systemsteuerelemente für dieses Objekt beeinflussen die Verarbeitung des Verwaltungsservers und des (der) Sicherheitsmanager(s) in der gesicherten Domäne.

Steuerelemente für die Replikationsverwaltung bestimmen, welche Prozesse zum Lesen oder Aktualisieren der Hauptberechtigungs-Policy-Datenbank zulässig sind, damit die Replikation ordnungsgemäß durchgeführt wird.

Zu den Steuerelementen und den zugeordneten Berechtigungen gehören:

| | Operation | Beschreibung |
|---|---|---|
| **v** | view | Hauptberechtigungsdatenbank lesen. |
| **m** | modify | Änderung der Replikationsdatenbank(en) berechtigen. |

Allen Policy Director-Servern, die eine lokale Replikation (Kopie) der Berechtigungsdatenbank verwalten — hierzu gehören alle Ressourcenmanager und Authorization Server — muss die Berechtigung view (**v**) für das Objekt **/Management/Replica** erteilt werden. Für den Replikationsprozess ist es erforderlich, dass diese Prozesse Einträge aus der Hauptberechtigungs-Policy-Datenbank anzeigen und auf sie zugreifen können. Bei der Policy Director-Installation wird jedem Server, der Zugriff auf die Berechtigungs-Policy-Datenbank benötigt, automatisch die Berechtigung read (lesen) erteilt.

Policy Director verwendet die Berechtigung modify (**m**) momentan nicht. Die Hauptberechtigungs-Policy-Datenbank kann nur durch den Web Portal Manager oder das Dienstprogramm **pdadmin** geändert werden. Diese Tools unterliegen anderen, feinkörnigeren Überprüfungen. Die Berechtigung modify ist für zukünftige Verwendung gedacht, wenn es möglich ist, den Verwaltungsserver zu replizieren (vervielfältigen).

## /Management/Users-Berechtigungen

Mit diesem Objekt können Verwaltungsbenutzer geschützte Benutzerkonten verwalten. Aktions-Tasks und zugehörige Berechtigungen:

| | Operation | Beschreibung |
|---|---|---|
| **d** | delete | Ein Benutzerkonto löschen.<br>`user delete` |
| **m** | modify | Benutzerkontodetails ändern.<br>`user modify authentication-mechanism`<br>`user modify account-valid`<br>`user modify gsouser`<br>`user modify description` |

| | Operation | Beschreibung |
|---|---|---|
| **N** | create | Einen neuen Benutzer erstellen und diesen Benutzer wahlweise einer Gruppe zuordnen. Gruppendaten aus der Benutzerregistrierungs-datenbank importieren.<br>`user create`<br>`user import` |
| **v** | view | Benutzerkonten auflisten und Benutzerkonto-details anzeigen.<br>`user list`<br>`user list-dn`<br>`user list-gsouser`<br>`user show`<br>`user show-dn`<br>`user show-groups` |
| **W** | password | Ein Benutzerkennwort zurücksetzen und überprü-fen.<br>`user modify password`<br>`user modify password-valid` |

Die Berechtigung W gestattet das Zurücksetzen von Kennwörtern und sollte Help-Desk-Administratoren erteilt werden, damit sie Benutzern helfen können, die ihr Kennwort vergessen haben. Diese Berechtigung gestattet einem Administrator, das vergessene Kennwort zurückzusetzen und dann mit dem Befehl **user modify password-valid** den Wert “no” (Nein) anzugeben. Hierdurch kann sich der Benutzer anmelden, und der Benutzer ist dann gezwungen, sofort ein neues Kennwort anzuwenden.

Die durch das Objekt /Management/Users erteilte Zugriffsberechtigung überschreibt alle Zugriffseinschränkungen, die durch ACLs der “Stellvertreterverwaltungs”-Policy unter /Management/Groups/ <*Gruppenname*> auferlegt werden.

## /Management/Groups-Berechtigungen

Mit diesem Objekt können Verwaltungsbenutzer Gruppen und Gruppenzugehörigkeiten verwalten. Aktions-Tasks und zugehörige Berechtigungen:

| | Operation | Beschreibung |
|---|---|---|
| **d** | delete | Eine Gruppe löschen.<br>`group delete` |
| **m** | modify | Gruppenbeschreibungen ändern. Einen Benutzer als Mitglied einer Gruppe entfernen.<br>`group modify description`<br>`group modify remove` |
| **N** | create | Eine neue Gruppe erstellen. Gruppendaten aus der Benutzerregistrierungsdatenbank importieren.<br>`group create`<br>`group import` |
| **v** | view | Gruppen auflisten und Gruppendetails anzeigen.<br>`group list`<br>`group list-dn`<br>`group show`<br>`group show-dn`<br>`group show-members` |
| **A** | add | Einen vorhandenen Benutzer einer Gruppe hinzufügen.<br>`group modify add` |

Die Berechtigung A ist in Ihrem Eintrag in der Zugriffssteuerungsliste für eine Gruppe erforderlich, damit Sie Ihrer Gruppe vorhandene Benutzer hinzufügen können. Mit dem Befehl **user create** (der die Berechtigung N erfordert) erstellen Sie neue Benutzer und fügen Sie wahlweise einer vorhandenen Gruppe hinzu.

Das Hinzufügen von vorhandenen Benutzern zu Ihrer Gruppe ist wirkungsvoll, da der Eigner einer Gruppe die Steuerung über alle Benutzer der Gruppe hat. Wenn Sie als Eigner der Gruppe auch über die Berechtigung delete (d) verfügen, können Sie diesen Benutzer aus der gesamten gesicherten Domäne löschen.

## /Management/GSO-Berechtigungen

Mit dem Containerobjekt **/Management/GSO** des geschützten Objektbereichs können Administratoren GSO-Verwaltungs-Tasks ausführen (wenn entsprechende Berechtigungen definiert sind).

| | Operation | Beschreibung |
|---|---|---|
| **m** | modify | `rsrcgroup modify`<br>`rsrccred modify` |
| **v** | view | `rsrc list`<br>`rsrcgroup list`<br>`rsrccred list`<br>`rsrc show`<br>`rsrcgroup show`<br>`rsrccred show` |
| **N** | create | `rsrc create`<br>`rsrcgroup create`<br>`rsrccred create`<br>`(alle oben aufgeführten Befehle erfordern außerdem m)` |
| **d** | delete | `rsrc delete`<br>`rsrcgroup delete`<br>`rsrccred delete`<br>`(alle oben aufgeführten Befehle erfordern außerdem m)` |

## Objekt- und Objektbereichsberechtigungen

Mit diesen Befehlen können Verwaltungsbenutzer neue Objekte und Objektbereiche verwalten. Aktions-Tasks und zugehörige Berechtigungen:

| | Operation | Beschreibung |
|---|---|---|
| **b** | browse | `objectspace list`<br>`objectspace writefile`<br>`object list`<br>`object listandshow`<br>`(erfordert zusätzlich v)` |
| **d** | delete | `objectspace delete`<br>`object delete`<br>`object modify set name`<br>`(erfordert zusätzlich m)` |
| **m** | modify | `objectspace create`<br>`objectspace readfile`<br>`object create`<br>`object modify` |
| **v** | view | `object listandshow`<br>`(erfordert zusätzlich b)`<br>`object show` |

# Standardverwaltungs-ACL-Policies

Die folgenden Standardverwaltungs-ACL-Policies werden als Basis für die Sicherung bestimmter Bereiche der gesicherten Domäne vorgeschlagen.

Sie können Einträge für Benutzer, Gruppen, Beliebige andere (Beliebige authentifizierte) und Nicht authentifizierte hinzufügen, um einen breiteren Steuerungsbereich zu erhalten und die Anforderungen Ihres geschützten Objektbereichs besser zu erfüllen.

Notieren Sie die Benutzer und Gruppen in jeder Zugriffssteuerungsliste (ACL), die über die Berechtigung control (**c**) verfügen. Benutzer und Gruppen mit der Berechtigung control sind “Eigner” der ACL und können die ACL-Einträge ändern.

## Standardstamm-ACL-Policy

Zu den Kerneinträgen der Standardstamm-ACL, **default-root**, gehören:

```
Gruppe iv-admin              Tcmdbva
Beliebige andere             T
Nicht authentifiziert        T
```

Die **Stamm**zugriffssteuerungsliste (Stamm-ACL) ist die Basis — alle können den Objektbereich durchqueren, aber keine anderen Aktionen ausführen. Normalerweise müssen Sie hier keine Änderung vornehmen. Ein Vorteil der Stamm-ACL liegt jedoch darin, dass einem einzelnen Benutzer oder einer einzelnen Gruppe schnell der Zugriff auf den gesamten Objektbereich verweigert werden kann.

Beispiel: Die **Stamm**-ACL enthält den folgenden Eintrag:

```
Benutzer john -----------------
```

Dieser Eintrag (keine Berechtigungen) bewirkt, dass **Benutzer john** das Stammcontainerobjekt nicht einmal durchqueren kann. Dieser Benutzer erhält überhaupt keinen Zugriff auf den geschützten Objektbereich — unabhängig von den Berechtigungen, die an einer untergeordneten Position in der Baumstruktur angegeben sind.

Dieses Verfahren können Sie auch auf den Objektbereich WebSEAL übertragen. Wenn Sie beispielsweise einem bestimmten Benutzer die Berechtigung traverse für Containerobjekte **/WebSEAL** entziehen, kann dieser Benutzer nicht auf den Objektbereich WebSEAL zugreifen — unabhängig von den Berechtigungen, die für Objekte in diesen Bereichen erteilt wurden.

## Standard-/WebSEAL-ACL-Policy

Zu den Kerneinträgen der WebSEAL-ACL, **default-webseal**, gehören:

```
Gruppe iv-admin            Tcmdbsvarxl
Gruppe webseal-servers     Tgmdbsrxl
Benutzer sec_master        Tcmdbsvarxl
Beliebige andere           Trx
Nicht authentifiziert      T
```

Bei der Installation wird diese Standardzugriffssteuerungsliste dem Containerobjekt **/WebSEAL** im Objektbereich zugeordnet.

Die Gruppe **webseal-servers** enthält einen Eintrag für jeden WebSEAL-Server in der gesicherten Domäne. Mit den Standardberechtigungen können die Server auf Browser-Anforderungen reagieren.

Die Berechtigung traverse gestattet die Erweiterung des Webbereichs wie im Web Portal Manager dargestellt. Die Berechtigung list ermöglicht dem Web Portal Manager, den Inhalt des Webbereichs anzuzeigen.

## Standard-/Management-ACL-Policy

Zu den Kerneinträgen der /Management-ACL, **default-management**, gehören:

```
Gruppe iv-admin            TcmdbsvatNWA
Gruppe ivmgrd-servers      Ts
Beliebige andere           Tv
```

Bei der Installation wird diese Zugriffssteuerungsliste (ACL) dem Containerobjekt **/Management** im Objektbereich zugeordnet.

## Standard-/Replica-ACL-Policy

Zu den Kerneinträgen der /Replica-ACL, **default-replica**, gehören:

```
Gruppe iv-admin            Tcbva
Gruppe ivmgrd-servers      m
Gruppe secmgrd-servers     mdv
Gruppe ivacld-servers      mdv
```

## Standard-/Config-ACL-Policy

Zu den Kerneinträgen der /Config-Management-ACL, **default-config**, gehören:

```
Gruppe iv-admin            TcmdbsvaN
Beliebige andere           Tv
Nicht authentifiziert      Tv
```

## Standard-/GSO-ACL-Policy

Zu den Kerneinträgen der /GSO-Management-ACL, **default-gso**, gehören:

```
Gruppe iv-admin            TcmdbvaN
Beliebige andere           Tv
Nicht authentifiziert      Tv
```

## Standard-/Policy-ACL-Policy

Zu den Kerneinträgen der /Policy-Management-ACL, **default-policy**, gehören:

```
Gruppe iv-admin            TcmdbvaN
Beliebige andere           Tv
Nicht authentifiziert      Tv
```



# Policies für geschützte Objekte verwenden

Der Policy Director-Berechtigungsservice trifft Entscheidungen über Zugriffsanforderungen für geschützte Objekte in der gesicherten Domäne. Die Entscheidung kann anhand von zwei Policy-Arten getroffen werden:

- ACL-Policies (ACL = Access Control List, Zugriffssteuerungs-liste)
- POP-Policies (POP = Protected Object Policies, Policies für geschützte Objekte)

Eine POP-Policy dient dazu, den durch die ACL-Policy erlaubten Operationen zusätzliche Bedingungen aufzuerlegen.

Beispiele für Zugriffsbedingungen:

- Berichtssatz im Prüfservice speichern
- Zugriff auf einen bestimmten Zeitraum beschränken

In diesem Kapitel wird beschrieben, wie POP-Policies konfiguriert und auf Objekte angewendet werden.

Stichwortindex:

- „POP-Policies - Einführung” auf Seite 106
- „POP-Attribute konfigurieren” auf Seite 109

# POP-Policies - Einführung

ACL-Policies stellen dem Berechtigungsservice Informationen zur Verfügung, mit denen eine positive oder eine negative Entscheidung bezüglich einer Zugriffsanforderung für ein geschütztes Objekt und für die Ausführung von Operationen mit diesem Objekt getroffen werden kann.

POP-Policies (POP = Protected Object Policies, Policies für geschützte Objekte) enthalten zusätzliche Bedingungen für die Anforderung, die zusammen mit der positiven Entscheidung zur ACL-Policy vom Berechtigungsservice zurück an den Ressourcenmanager (z. B. WebSEAL) gesendet werden. Der Ressourcenmanager ist für die Durchsetzung der POP-Bedingungen zuständig.

Die folgende Tabelle enthält die verfügbaren Attribute für eine Policy Director POP-Policy:

| **Erzwungen durch Policy Director Base** | | |
|---|---|---|
| **POP-Attribut** | **Beschreibung** | **pdadmin pop-Befehle** |
| **Name** | Name der Policy. Dies wird der <*POP-Name*> in den **pdadmin pop**-Befehlen. | `create`<br>`delete` |
| **Beschreibung** | Beschreibender Text für die Policy. Erscheint im **pop show**-Befehl. | `modify set description` |
| **Warnungsmodus** | Methode zum Testen von ACL- und POP-Policies für Administratoren. | `modify set warning` |
| **Prüfungsstufe** | Gibt die Art der Prüfung an: Alle, Keine, Zulassen, Verweigern, Fehler. | `modify set audit-level` |
| **Zugriffszeit** | Tages- und Zeitangaben für einen erfolgreichen Zugriff auf ein geschütztes Objekt. | `modify set tod-access` |
| **Erweiterte Attribute** | Gibt ergänzende Datenfelder an. | `modify set attribute`<br>`modify delete attribute`<br>`list attribute`<br>`show attribute` |

| Erzwungen durch Ressourcenmanager (z. B. WebSEAL) | | |
|---|---|---|
| **POP-Attribut** | **Beschreibung** | **pdadmin pop-Befehle** |
| **Sicherungsstufe** | Gibt den Grad des Datenschutzes an: Keine, Integrität, Zugriffscode. | `modify set qop` |
| **Policy für IP-Endpunkt-Authentifizierungsmethode** | Gibt Authentifizierungsanforderungen für den Zugriff von externen Netzen an. | `modify set ipauth add`<br>`modify set ipauth remove`<br>`modify set ipauth anyotherw` |

## Hinweise zu POP-Policies:

- ’Zugriffszeit’ und ’Policy für IP-Endpunkt-Authentifizierungsmethode’ schränken den Zugriff auf das Objekt ein.
- ’Prüfungsstufe’ und ’Sicherungsstufe’ informieren den Berechtigungsservice darüber, dass zusätzliche Services erforderlich sind, wenn der Zugriff auf das Objekt gestattet wird.
- ’Warnungsmodus’ stellt eine Möglichkeit, ACL- und POP-Policies vor ihrer Aktivierung zu testen, zur Verfügung.

**Anmerkung:** Die in früheren Versionen von Policy Director durch die Berechtigungen P, I und A angegebene Sicherungsstufe und die angegebenen Prüfregeln werden jetzt in POP-Policies angegeben.

## POP-Policies erstellen und löschen

POP-Policies funktionieren ähnlich wie ACL-Policies — Sie erstellen und konfigurieren eine POP-Policy und ordnen sie dann Objekten im geschützten Objektbereich zu.

POP-Policies werden wie ACL-Policies übernommen. Sowohl POP-Policies als auch ACL-Policies werden in der Hauptberechtigungsdatenbank gespeichert, die durch den Verwaltungsserver gesteuert wird.

## POP-Policy erstellen und auflisten

```
pdadmin> pop create <POP-Name>
```

Zum Beispiel:

```
pdadmin> pop create test
pdadmin> pop list
       test
```

Die neue POP-Policy enthält folgende Standardeinstellungen:

```
pdadmin> pop show test
       Policy für geschütztes Objekt:  test
       Beschreibung:
       Warnung:  nein
       Prüfungsstufe:  keine
       Sicherungsstufe:  keine
       Zugriffszeit: Son, Mon, Die, Mit, Don, Fre, Sam:
           anytime:local
       Policy für IP-Endpunkt-Authentifizierungsmethode
           Anderes Netz 0
```

## POP-Policy löschen

```
pdadmin> pop delete <POP-Name>
```

Zum Beispiel:

```
pdadmin> pop delete test
pdadmin> pop list
pdadmin>
```

## POP-Beschreibung ändern und anzeigen

```
pdadmin> pop modify <POP-Name> set description <Beschreibung>
```

**Anmerkung:** Die Beschreibung muss in doppelte Anführungszeichen eingeschlossen werden, wenn sie aus mehreren Wörtern besteht.

Zum Beispiel:

```
pdadmin> pop modify test set description "Test POP"
pdadmin> pop show test
       Policy für geschütztes Objekt:  test
       Beschreibung:  Test POP
       Warnung:  nein
       Prüfungsstufe:  keine
       Sicherungsstufe:  keine
```

```
Zugriffszeit: Son, Mon, Die, Mit, Don, Fre, Sam:
    anytime:local
Policy für IP-Endpunkt-Authentifizierungsmethode
    Anderes Netz 0
```

## POP-Attribute auf geschützte Objekte anwenden

POP-Policies werden wie ACL-Policies auf Objekte angewendet.

### POP-Policy einem Objekt zuordnen

Die Syntax für das Zuordnen einer POP-Policy zu einem Objekt lautet:

```
pdadmin> pop attach <Objektname> <POP-Name>
```

Zum Beispiel:

```
pdadmin> pop attach /WebSEAL/serverA/index.html test
```

### Herausfinden, wo eine POP-Policy zugeordnet ist

```
pdadmin> pop find test
       /WebSEAL/serverA/index.html
```

### POP-Policy löschen

Die Syntax für das Freigeben einer POP-Policy von einem Objekt lautet:

```
pdadmin> pop detach <Objektname>
```

Zum Beispiel:

```
pdadmin> pop detach /WebSEAL/serverA/index.html
```

# POP-Attribute konfigurieren

- Warnungsmodusattribut
- Prüfungsstufenattribut
- Zugriffszeitattribut
- Sicherungsstufenattribut
- IP-Endpunkt-Authentifizierungsmethodenattribut

## Warnungsmodusattribut

Das Warnungsattribut gestattet einem Sicherheitsadministrator, die Richtigkeit der Berechtigungs-Policy, die für den geschützten Objektbereich definiert ist, zu prüfen.

Wird für das Warnungsattribut “yes” (Ja) angegeben, kann jeder Benutzer jede Aktion für das Objekt, dem die POP-Policy zugeordnet ist, ausführen. Für ein Objekt ist jeder Zugriff zulässig, auch wenn durch die ACL-Policy, die dem Objekt zugeordnet ist, der Zugriff verweigert wird.

Es werden Protokolleinträge generiert, in denen die Ergebnisse aller ACL-Policies, für die der Warnungsmodus definiert ist, im gesamten Objektbereich erfasst werden. Das Prüfprotokoll zeigt, welches Ergebnis eine Berechtigungsentscheidung gehabt hätte, wenn für das Warnungsattribut “no” (Nein) definiert worden wäre. Der Administrator kann auf diese Weise feststellen, ob eine Policy definiert ist und korrekt eingesetzt wird.

```
pdadmin> pop modify <POP-Name> set warning {yes|no}
```

Zum Beispiel:

```
pdadmin> pop modify test set warning yes
```

## Prüfungsstufenattribut

Das POP-Attribut ’Prüfungsstufe’ ersetzt die ACL-Berechtigung “A”, mit der in früheren Versionen von Policy Director die Prüfung aktiviert wurde. Die POP-Prüfungsstufe verfügt über die zusätzliche Fähigkeit, eine Prüfungsstufe anzugeben.

Wenn die Prüfung beispielsweise so definiert ist, dass nicht erfolgreiche Ereignisse aufgezeichnet werden, können Sie mit Hilfe der Ergebnisse eine ungewöhnliche Anzahl fehlgeschlagener Zugriffsversuche für eine bestimmte Ressource feststellen.

Protokolleinträge werden in einem XML-Standardformat gespeichert, das eine einfache Syntaxanalyse zum Extrahieren der erforderlichen Informationen gestattet.

Siehe „Prüfprotokolldateien” auf Seite 176.

```
pdadmin> pop modify <POP-Name> set audit-level
{all|none|<Prüfungsstufenliste>
```

| Prüfungsstufenliste | |
|---|---|
| **Wert** | **Beschreibung** |
| **permit** | Alle Anforderungen für ein geschütztes Objekt mit erfolgreichem Zugriff prüfen. |
| **deny** | Alle Anforderungen für ein geschütztes Objekt mit Zugriffsverweigerung prüfen. |
| **error** | Alle intern generierten Fehlernachrichten, die aus einer Zugriffsverweigerung für das geschützte Objekt resultieren, prüfen. |

Sie können eine beliebige Kombination dieser drei Werte anwenden. Wenn Sie mehrere Werte angeben, müssen Sie ein Komma als Trennzeichen verwenden.

Zum Beispiel:

```
pdadmin> pop modify test set audit-level permit,deny
```

## Zugriffszeitattribut

Das POP-Attribut 'Zugriffszeit' gestattet bestimmte zeitliche (Tag und Uhrzeit) Bedingungen für den Zugriff auf ein geschütztes Objekt festzulegen. Diese Bedingung ist nützlich, um den Zugriff auf Informationen, die regelmäßig zu Änderungs- und Aktualisierungszwecken gesperrt werden müssen, einzuschränken.

Es gibt ein ACL-Policy-Berechtigungs-Bit ("B"), das die zeitlichen Zugriffsbedingungen für ein Objekt überschreibt. Diese Berechtigung sollte nur von einem Systemadministrator verwendet werden, der immer uneingeschränkten Zugriff auf den geschützten Objektbereich benötigt.

```
pop modify <POP-Name> set tod-access <Uhrzeit>
```

Zu dem Uhrzeitargument gehören ein Tages- und ein Zeitbereich, und es hat folgendes Format:

```
<{anyday|weekday|<Tagesliste>}>:
<{anytime|<Zeitspezifikation>-<Zeitspezifikation>}>
[:{utc|local}]
```

Die Variable **Tagesliste** kann eine Kombination aus folgenden Angaben sein:

```
Mon,Die,Mit,Don,Fre,Sam,Son
```

Die Bereichsvariable **Zeitspezifikation** muss im 24-Stunden-Format wie folgt angegeben werden:

```
hhmm-hhmm
```

Zum Beispiel:

```
0700-1945
```

Die optionale Zeitzone für den Server (nicht für den Client) ist standardmäßig **local**.

Zum Beispiel:

```
pdadmin> pop modify test set tod-access Mon,Die,Fre:1315-1730
```

## Sicherungsstufenattribut

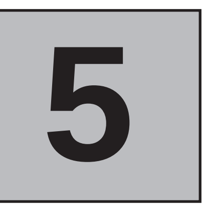
Das POP-Attribut ’Sicherungsstufe’ gestattet die Angabe in WebSEAL, welche Datenschutzstufe erforderlich ist, wenn eine Operation für ein Objekt ausgeführt wird.

Detaillierte Informationen zu diesem POP-Attribut finden Sie im *Tivoli SecureWay Policy Director WebSEAL Administratorhandbuch*.

## IP-Endpunkt-Authentifizierungsmethodenattribut

Mit dem POP-Attribut für die IP-Endpunkt-Authentifizierungsmethode können Sie Authentifizierungsstufen-Policy (Erweiterung) und netzbasierte Authentifizierungs-Policy konfigurieren.

Detaillierte Informationen zu diesem POP-Attribut finden Sie im *Tivoli SecureWay Policy Director WebSEAL Administratorhandbuch*.



# Verwaltungs-Tasks delegieren



Policy Director gestattet Systemadministratoren das Delegieren von Zuständigkeiten für die Verwaltung der gesicherten Domäne an untergeordnete Administratoren. Diese Funktion ist für eine erfolgreiche Verwaltung sehr großer Domänen, die aus zahlreichen Abteilungen bestehen und folglich zahlreiche Gruppen, Benutzer und Ressourcen aufweisen, unerlässlich.

Policy Director unterstützt zwei Arten der Stellvertreterverwaltung:

- Stellvertreterverwaltung von Ressourcen in Unterbereichen des Objektbereichs

  Die Verwaltungsberechtigung ist auf einen Abschnitt des Objektbereichs beschränkt.

- Stellvertreterverwaltung von Gruppen und Benutzern

  Die Verwaltungsberechtigung ist auf einen Teil der Benutzer beschränkt.

Stichwortindex:

# Stellvertreterverwaltung im Objektbereich

Das Verteilen der Verwaltungszuständigkeit innerhalb einer gesicherten Domäne wird als Stellvertreterverwaltung bezeichnet. Die Stellvertreterverwaltung wird normalerweise durch wachsende Anforderungen eines großen Standorts mit vielen verschiedenen Unternehmens- und Ressourcenbereichen erforderlich.

In der Regel kann ein großer Objektbereich in Bereiche unterteilt werden, die diese Abteilungen oder Unternehmensbereiche darstellen. Die einzelnen Bereiche der Domäne werden normalerweise besser durch einen Manager organisiert und verwaltet, der mit den Aufgaben und Anforderungen des betreffenden Bereichs vertraut ist.

In einer gesicherten Domäne von Policy Director ist das Konto **sec_master** für LDAP zunächst das einzige Konto mit Verwaltungsberechtigung. Als **sec_master** können Sie Verwaltungskonten erstellen und diesen Konten entsprechende Steuerelemente für bestimmte Bereiche des Objektbereichs zuordnen.

## Objektbereich für die Stellvertreterverwaltung strukturieren

Gliedern Sie Ihren Objektbereich in bestimmte Bereiche auf, in denen untergeordnete Verwaltungsaktivitäten, die speziell für diesen Unterbereich gelten, ausgeführt werden können.

In dem folgenden Beispiel benötigen die beiden Bereiche ’Technischer Server’ und ’Veröffentlichungen’ des Objektbereichs separate Verwaltungssteuerung. Die Steuerung dieser Regionen beginnt mit dem Stamm (Root) jedes Bereichs und weitet sich auf alle untergeordneten Objekte aus.

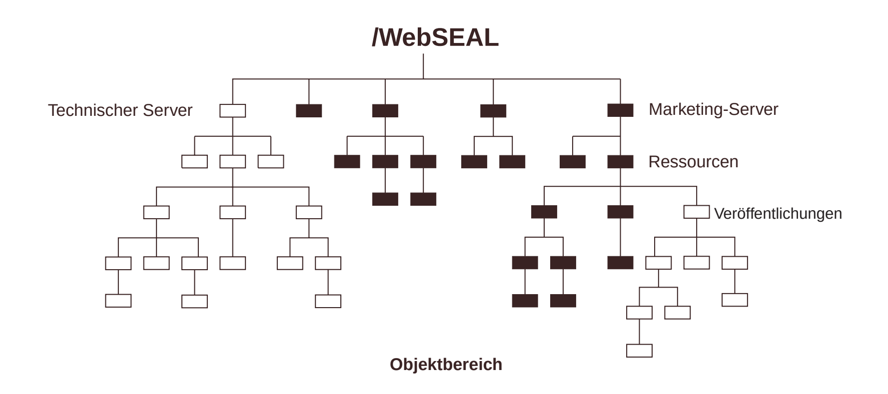



*Abbildung 24. Objektbereich für die Stellvertreterverwaltung strukturieren*



# Standardverwaltungsbenutzer und -gruppen

Bei der Installation stellt Policy Director mehrere wichtige Verwaltungsgruppen zur Verfügung. Diese Benutzer und Gruppen erhalten standardmäßig spezielle Berechtigungen für die Steuerung und Verwaltung aller Operationen in der gesicherten Domäne. (Diese Standardsicherheits-Policy wird durch die Zugriffssteuerungslisten (ACLs), die während der Installation erstellt werden, definiert.)

Die folgenden Abschnitte beschreiben ausführlich die spezifischen Berechtigungsklassen, die den einzelnen Benutzern und Gruppen während der Installation zugeordnet werden. Der Administrator kann diese Berechtigungen später anpassen, um auf geänderte Verwaltungs-Policies zu reagieren.

## Benutzer sec_master (LDAP)

Dieser Benutzer stellt den Administrator der gesicherten Domäne dar, dem uneingeschränkte Berechtigungen für alle Operationen innerhalb der gesicherten Domäne erteilt werden.

Diese Policy kann mit dem Anwachsen des Objektbereichs durch Delegieren von Verwaltungsberechtigungen auf andere Benutzer und Entziehen bestimmter (oder aller) Berechtigungen von **sec_master** geändert werden.

### Gruppe iv-admin

Diese Gruppe stellt die Administratorgruppe dar. Wie **sec_master** betrachtet die Standard-Policy alle Mitglieder dieser Gruppe als Administratoren der gesicherten Domäne. Alle Standard-ACLs erteilen Benutzer **sec_master** und Gruppe **iv-admin** exakt dieselben Berechtigungen.

Sie können Benutzer einfach durch Hinzufügen zur Gruppe **iv-admin** in eine Verwaltungsberechtigungsklasse einfügen. Die Gefahr hierbei besteht darin, dass ein Benutzer, der Mitglied dieser Gruppe wird (mit den Standard-ACLs), uneingeschränkte Berechtigungen für alle Operationen für alle Objekte im gesamten Namensbereich erhält.

Die Standard-Policy für diese Gruppe kann durch Delegieren von Verwaltungsberechtigungen an andere Benutzer und durch Entziehen von Verwaltungsberechtigungen (ganz oder teilweise) von der Gruppe **iv-admin** geändert werden.

### Gruppe ivmgrd-servers

Diese Gruppe enthält den Verwaltungsserver. Policy Director erfordert, dass exakt ein Verwaltungsserver in der gesicherten Domäne vorhanden ist. Daher enthält diese Gruppe nur diesen einen Eintrag.

Da die meisten Verwaltungsanforderungen durch die Konsole über den Verwaltungsserver auf dem Zielserver ausgeführt werden, benötigt der Verwaltungsserver die Berechtigung, die Anforderung auf dem Zielserver auszuführen. Aus diesem Grund wird dieser Gruppe die Berechtigung server administration (**s**) in der Standardverwaltungs-ACL und die Berechtigung list (**l**) im gesamten Webbereich erteilt.

### Gruppe webseal-servers

Diese Gruppe enthält alle WebSEAL-Server in der gesicherten Domäne. Die WebSEAL-Standard-ACL erteilt diesen Servern die vollständige Gruppe der HTTP-spezifischen Berechtigungen und die Stellvertreterberechtigung. Diese Policy gestattet allen WebSEAL-Servern die Junction zu allen anderen WebSEAL-Servern zu überqueren. Eine Änderung dieser Policy könnte diese Berechtigungen auf einer Serverbasis erteilen.

## Verwaltungsbenutzer erstellen

Sie können Verwaltungskonten mit verschiedenen Zuständigkeitsgraden erstellen. Die Zuständigkeit wird durch strategische Positionierung von Verwaltungs-ACLs an Administratoren delegiert. Die folgende Liste illustriert mögliche Verwaltungsberechtigungsklassen:

- **ACL-Verwaltungszuständigkeiten**

  Der ACL-Administrator kann den Namensbereich eines geschützten Objekts ganz oder teilweise steuern, je nachdem, an welcher Position sich die Verwaltungs-ACL befindet. Der ACL-Eintrag des Administrators könnte die Berechtigungen **b**, **a** und **T** sowie beliebige weitere Berechtigungen, die für Operationen für Objekte in diesem Bereich geeignet sind, enthalten.

  Der Administrator kann mit Hilfe der Management Console ACLs Objekten in dem angegebenen Namensbereich zuordnen (Berechtigung attach (**a**)) und dabei die vorhandene Gruppe der ACL-Schablonen verwenden. Dieser Administrator hat keine Berechtigung zum Erstellen, Ändern oder Löschen von ACL-Schablonen.

- **ACL-Policy-Zuständigkeiten**

  Der ACL-Policy-Administrator sollte für die Steuerung der Erstellung und Änderung aller ACL-Schablonen, die in der gesicherten Domäne verwendet werden, verantwortlich sein. Dem ACL-Policy-Administrator sollten die Berechtigungen **d**, **b**, **m** und **v** für das Objekt /Management oder /Management/ACL erteilt werden.

Dieser ACL-Policy-Administrator kann neue ACL-Schablonen erstellen (**m**). Als Ersteller einer neuen Schablone wird der Administrator standardmäßig zum ersten Eintrag in der neuen ACL-Schablone, und er erhält die Berechtigungen **abcT**. Die Berechtigung control (**c**) gibt dem Administrator effektiv das Eigentumsrecht für die Zugriffssteuerungsliste (ACL) und folglich die Möglichkeit, die ACL zu ändern.

Als Eigner der ACL kann der Administrator die Berechtigung delete (**d**), die in der Verwaltungs-ACL erteilt wird, verwenden, um die ACL aus der Schablonenliste zu entfernen. Sie können eine ACL-Schablone nur löschen, wenn Sie der Eigner dieser ACL sind.

- **Serververwaltungszuständigkeiten**

  Diesem Administrator werden die Berechtigungen **d**, **m**, **s** und **v** für das Objekt /Management/Server erteilt. Dieser Administrator kann Operationen ausführen, die die Policy Director-Server betreffen.

- **Berechtigungsaktionszuständigkeiten**

  Diesem Administrator werden die Berechtigungen **d** und **m** für das Objekt /Management/Action erteilt. Dieser Administrator kann alle Berechtigungen, die für Anwendungen anderer Hersteller erstellt wurden, erstellen oder löschen.

## Beispielverwaltungs-ACL-Schablonen

Das folgende Beispiel zeigt, wie ein Benutzer Verwaltungsberechtigungen erlangt.

- Die folgende Zugriffssteuerungsliste (ACL) für /WebSEAL erteilt **Benutzer adam** Verwaltungsberechtigungen:

```
Benutzer sec_master                        abcTdmlrx
Gruppe iv-admin                            abcTdmlrx
Gruppe webseal-servers                     gTdmlrx
Gruppe ivmgrd-servers                      Tl
Benutzer adam                              abcTdmlrx
Beliebige andere                           Trx
Nicht authentifiziert                      Trx
```

## Beispiel: Stellvertreterverwaltung

Für einen großen Objektbereich ist es unter Umständen erforderlich, dass viele Verwaltungsbenutzer verschiedene Unterbereiche verwalten. In diesem Szenario müssen die Zugriffssteuerungslisten (ACLs) für die Verzeichnisse in dem Pfad zu jedem dieser Bereiche Einträge für jedes Konto mit der Berechtigung traverse enthalten. Bei einem Standort mit vielen Verwaltungsbenutzern könnten diese ACLs eine lange Liste mit Einträgen, die all diese Verwaltungskonten darstellen, enthalten.

Das Problem der zahlreichen ACL-Einträge für Administratoren kann mit folgendem Verfahren gelöst werden:

1. Erstellen Sie ein Verwaltungsgruppenkonto.
2. Fügen Sie alle neuen Verwaltungsbenutzer dieser Gruppe hinzu.
3. Fügen Sie diese Gruppe als ACL-Eintrag (mit Berechtigung traverse) den Verzeichnissen hinzu, die zu den einzelnen Unterbereichen, für die Stellvertreterverwaltung erforderlich ist, führen.
4. Fügen Sie an jeder Stamm-ACL eines Bereichs den entsprechenden Verwaltungsbenutzereintrag (mit den Berechtigungen **b**, **c**, **T** sowie anderen angemessenen Berechtigungen) hinzu.
5. Der Administrator kann jetzt den ACL-Eintrag der Verwaltungsgruppe (und jeden anderen Eintrag) aus dem Stamm (Root) entfernen.

   Jetzt hat nur dieser Benutzer die Steuerung über den Stamm und alle untergeordneten Objekte.

In dem folgenden Beispiel enthält die Gruppe **iv-admin** alle Verwaltungsbenutzer. Der Benutzer **pub-manager** ist Mitglied dieser Gruppe und verfügt daher über die erforderliche Berechtigung traverse, um auf das Verzeichnis `Veröffentlichungen` zuzugreifen.

Das Verzeichnis `Veröffentlichungen` enthält den Benutzereintrag **pub-manager** in seiner Zugriffssteuerungsliste (ACL).

Da **pub-manager** der Stellvertreteradministrator dieses Bereichs ist (mit den entsprechenden Berechtigungen), kann **pub-manager** das Gruppenkonto **iv-admin** (und alle anderen ACL-Einträge) aus der ACL für *Veröffentlichungen* entfernen, um die vollständige Steuerung über diesen Unterbereich des Webbereichs zu erhalten.

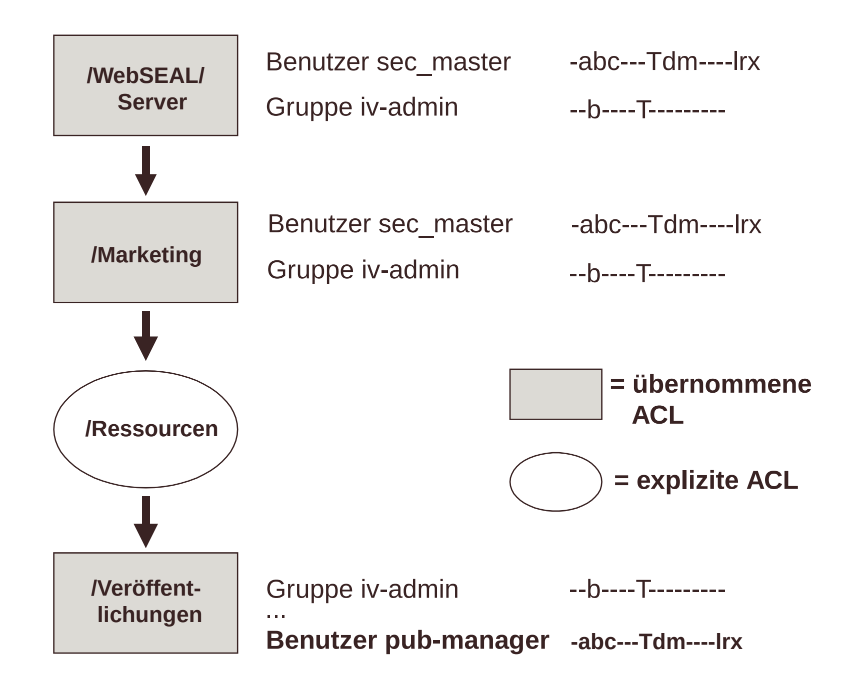



*Abbildung 25. Stellvertreterverwaltungsbeispiel*

## Gruppenverwaltung delegieren

Policy Director gestattet Systemadministratoren das Delegieren von Zuständigkeiten für die Verwaltung der gesicherten Domäne an untergeordnete Administratoren. Diese Funktion ist für eine erfolgreiche Verwaltung sehr großer Domänen, die aus zahlreichen Abteilungen bestehen und folglich zahlreiche Gruppen, Benutzer und Ressourcen aufweisen, unerlässlich.

Für die Verwaltung umfangreicher oder komplexer Benutzergruppen können Sie die Verwaltung bestimmter Benutzergruppen an untergeordnete Administratoren delegieren. Wenn ein Administrator die Policy-Verwaltungssteuerung für eine Gruppe erhält, hat dieser Administrator die Policy-Verwaltungssteuerung für die Benutzer in dieser Gruppe.

Stellvertretergruppenverwaltung definiert folgendes:

- Wer die Verwaltungszuständigkeit für eine bestimmte Gruppe (und die Benutzer in dieser Gruppe) besitzt
- Die Stufe der Gruppen- und Benutzersteuerung, die dieser Administrator erhält

In diesen Erläuterungen bezieht sich der Begriff “Administrator” auf die Zuständigkeiten und Steuerelemente, die ein ansonsten normaler Benutzer erhält. Ein Administrator mit Stellvertreterpflichten ist ein normaler Benutzer mit zusätzlichen Möglichkeiten, bestimmte Verwaltungs-Tasks auszuführen.

Das Definieren einer Stellvertretergruppenverwaltung erfordert folgende Bedingungen:

1. Festlegen einer logischen und praktischen Hierarchie der Benutzer und Benutzerarten, die zur gesicherten Domäne gehören
2. Erstellen von Gruppencontainerobjekten, die diese Hierarchie widerspiegeln
3. Erstellen entsprechender Gruppen innerhalb dieser Containerobjekte
4. Strategisches Zuordnen von ACL-Policies, die den Administratorbenutzereintrag enthalten
5. Zuordnen der spezifischen Berechtigungen, die für die Ausführung der erforderlichen Tasks benötigt werden, zu diesem Administratorbenutzereintrag

## Gruppencontainerobjekte erstellen

Der Bereich /Management des Policy Director-Objektbereichs verfügt standardmäßig über ein Containerobjekt /Groups, mit dem Sie die Hierarchie der Gruppen in Ihrer gesicherten Domäne aufbauen können.

Containerobjekte sind Strukturelemente, mit denen Sie eine aus begrenzten funktionalen Bereichen bestehende Hierarchie für den Objektbereich aufbauen können. Gruppencontainerobjekte gestatten Ihnen, bestimmte Kategorien der Gruppenarten zu definieren. Sie erstellen tatsächliche Gruppen innerhalb jedes einzelnen Gruppencontainerobjekts.

Ein neues Gruppencontainerobjekt erstellen Sie mit dem Befehl **pdadmin object create**:

```
pdadmin> object create <Objektname> <Beschreibung> <Art>
ispolicyattachable {yes|no}
```

| Argument | Beschreibung |
|---|---|
| **Objektname** | Vollständiger Pfad und Name des neuen Gruppencontainerobjekts. Der Pfad muss mit /Management/Groups beginnen. |
| **Beschreibung** | Beliebige Zeichenfolge, die das Objekt beschreibt. Diese Informationen erscheinen im Befehl **object show**. |
| **Art** | Das Argument 'Art' gibt das Grafiksymbol an, das diesem Objekt zugeordnet ist und von der Management Console angezeigt wird. Die Arten liegen im Bereich von 0-16 (siehe Tabelle unten). Die Art 14 ist für Containerobjekte geeignet. |
| **ispolicyattachable** | |
| | Legt fest, ob Sie diesem Objekt eine ACL-Policy zuordnen können. |

| Objektarten | |
|---|---|
| 0 – unbekannt<br>1 – gesicherte Domäne<br>2 – Datei<br>3 – ausführbares Programm<br>4 – Verzeichnis<br>5 – Junction<br>6 – WebSEAL-Server<br>7 – nicht verwendet<br>8 – nicht verwendet | 9 – HTTP-Server<br>10 – nicht vorhandenes Objekt<br>11 – Containerobjekt<br>12 – Blattobjekt<br>13 – Port<br>14 – Anwendungscontainerobjekt<br>15 – Anwendungsblattobjekt<br>16 – Verwaltungsobjekt<br>17 – nicht verwendet |

Zum Beispiel:

```
pdadmin> object create /Management/Groups/Travel "Containerobjekt
Travel" 10 ispolicyattachable yes
```

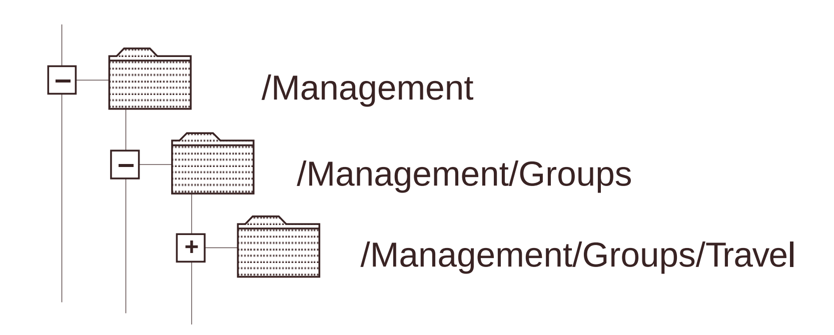



*Abbildung 26. Gruppencontainerobjekt*

Ein Gruppencontainerobjekt können Sie auch mit dem Befehl **pdadmin group create** erstellen. Siehe „Gruppen erstellen” auf Seite 124.

## Gruppen erstellen

Verwenden Sie den Befehl **pdadmin group create**, um eine neue Gruppe zu erstellen und diese wahlweise in ein Gruppencontainer-objekt einzufügen. Wenn das Containerobjekt noch nicht vorhanden ist, wird es automatisch erstellt.

```
pdadmin> group create <Gruppenname> <dn> <cn> [Gruppencontainer]
```

| Argument | Beschreibung |
|---|---|
| **Gruppenname** | Name des neuen Gruppenobjekts. |
| **dn** | Registrierter Name für die neue Gruppe. |
| **cn** | Allgemeiner Name für die neue Gruppe. |
| **Gruppen-container** | Relativer Pfadname für das Gruppencontainerobjekt, in dem sich diese neue Gruppe befinden soll. Wird kein Gruppencontainerobjekt angegeben, wird die Gruppe in /Management/Groups aufgenommen. |

- Alle neuen Gruppencontainerobjekte, die Sie erstellen, erscheinen unter dem Standardcontainer /Management/Groups. Soll ein Container auf einer anderen untergeordneten Ebene erstellt werden, müssen Sie für das Argument **Gruppencontainer** einen relativen Pfadnamen angeben.
- Bei Verwendung des Befehls **group create** ist es nicht möglich, ein Gruppencontainerobjekt ohne eine Gruppe zu erstellen.
- Um dem Objektbereich eine neue Gruppe hinzufügen zu können, muss der Administrator über die Berechtigung create (N) in der Zugriffssteuerungsliste (ACL), die für das zugeordnete Gruppencontainerobjekt gilt, verfügen.

  Wird kein Gruppencontainerobjekt angegeben, muss der ACL-Eintrag des Administrators (mit der Berechtigung create) in der ACL angegeben werden, die für den Container /Management/Groups gilt.

  Bei der Installation definiert eine einzelne Standard-ACL (default-management) — die /Management zugeordnet ist — die Berechtigungen für alle Gruppen und Gruppencontainer. Diese Steuerung müssen Sie durch Hinzufügen entsprechender expliziter ACLs anpassen.

- Sie können mehrere Gruppen einem einzelnen Gruppencontainer hinzufügen.

  Die Zugriffssteuerungsliste (ACL) für das Gruppencontainerobjekt steuert durch Übernahme alle Gruppen, die sich unter dem Containerobjekt befinden. Das Containerobjekt und seine Gruppen sind jetzt die Domäne des Administrators mit den Stellvertreterzuständigkeiten.

- Die Position einer neuen Gruppe im Objektbereich wird bei der Erstellung festgelegt.

  Nach der Erstellung einer Gruppe kann ihre Position nur geändert werden, indem die Gruppe aus dem Objektbereich (aber nicht LDAP) gelöscht und dann an eine neue Position importiert wird (Benutzer in der Gruppe bleiben erhalten).

Zum Beispiel:

```
pdadmin> group create group1 "cn=travel,c=us" Group1 Travel

pdadmin> group create group2 "cn=travel,c=us" Group2 Travel
```



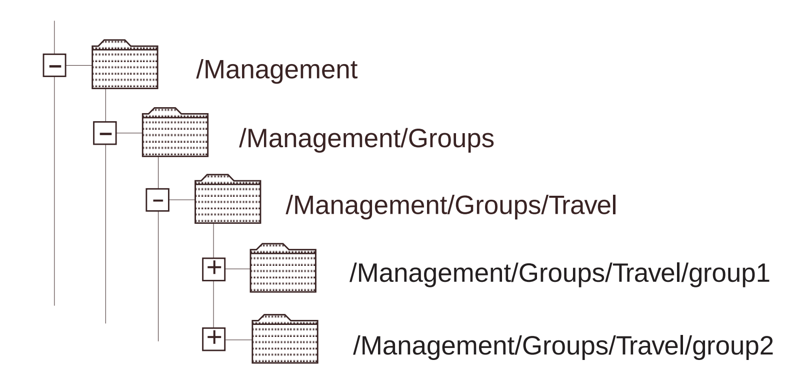



*Abbildung 27. Neue Gruppen unter einem bestimmten Gruppencontainer erstellen*

## ACL-Policies, die die Gruppenverwaltung betreffen

Die Berechtigung zum Steuern einer Benutzergruppe erhalten Sie durch Zuordnen einer entsprechenden Zugriffssteuerungsliste (ACL) zum Gruppenobjekt oder Gruppencontainerobjekt.

Die ACL, die durch einen übergeordneten Systemadministrator erstellt und zugeordnet wird, sollte die entsprechenden Berechtigungen für die Aktionen, die der Stellvertreteradministrator der Gruppe(n) ausführen muss, enthalten.

Wenn sich die Gruppe unter dem Abschnitt /Management/Groups des Objektbereichs befindet, muss die ACL /Management/Groups oder der Gruppe selbst zugeordnet werden.

Wenn sich die Gruppe unter dem Gruppencontainerobjekt befindet, muss die ACL dem Gruppencontainerobjekt oder der Gruppe selbst zugeordnet werden. Wenn Sie die ACL dem Containerobjekt /Management/Groups zuordnen, wirkt sich die ACL auf alle anderen untergeordneten Gruppencontainer im Objektbereich aus.

Die ACL, die einer dieser Positionen zugeordnet wird (oder übernommen wird), legt folgendes fest:

- Wer das Gruppenobjekt und die Benutzer in der Gruppe steuert
- Welche Aktionen für die Gruppe und ihre Benutzer ausgeführt werden können

Beispielsweise definiert in Abb. 27 auf Seite 125 eine ACL für /Management/Groups/Travel Berechtigungen zur Steuerung von group1 und group2.

Die folgenden Operationen und ACL-Berechtigungen sind für die Gruppenverwaltung geeignet:

| Operation | Berechtigung |
|---|---|
| erstellen (neue Gruppe) importieren (Gruppendaten aus der Benutzerregistrierungsdatenbank) | **N** (create) |
| löschen (eine Gruppe) | **d** (delete) |
| anzeigen (Gruppendetails) | **v** (view) |

| Operation | Berechtigung |
|---|---|
| ändern (Gruppenbeschreibung) | **m** (modify) |
| hinzufügen (vorhandenen Benutzer einer Gruppe) | **A** (add) |
| entfernen (Benutzer aus der Gruppe) | **A** (add) |

Diese Operationen können Sie mit den entsprechenden Befehlen des Dienstprogramms **pdadmin** ausführen.

### Anmerkungen:

- Die Berechtigung create (N) muss sich in einer Zugriffssteuerungsliste (ACL) befinden, die /Management/Groups zugeordnet ist, oder in einem Gruppencontainerobjekt.
- Alle anderen aufgeführten Berechtigungen können sich in einer ACL, die /Management/Groups zugeordnet ist, in einem Gruppencontainerobjekt oder im Gruppenobjekt selbst befinden.
- Die Berechtigung add (A) ist sehr mächtig, weil Sie mit ihr einen beliebigen vorhandenen Benutzer in Ihrer Gruppe hinzufügen können.

  Wenn ein außenstehender Benutzer in eine Gruppe aufgenommen wird, erhält der Administrator dieser Gruppe die Steuerung über diesen Benutzer (und kann den Benutzer mit Administratoren anderer Gruppen, in denen dieser Benutzer Mitglied ist, gemeinsame steuern).

  Diese Berechtigung sollte nur übergeordneten Systemadministratoren erteilt werden, die für Benutzer- und Gruppenorganisation sowie Unternehmens-Policy verantwortlich sind.

## ACL-Policies, die die Benutzerverwaltung betreffen

Der Gruppenadministrator kann eine Aktion für einen Benutzer ausführen, wenn er über die entsprechende Berechtigung verfügt, die in einer der Gruppen, zu denen dieser Benutzer gehört, definiert ist.

Die folgenden Operationen und ACL-Berechtigungen sind für die Benutzerverwaltung geeignet:

| Operation | Berechtigung |
|---|---|
| erstellen (neuen Benutzer in der angegebenen Gruppe) importieren (Benutzerdaten aus der Benutzerregistrierungsdatenbank) | **N** (create) |
| löschen (einen Benutzer) | **d** (delete) |
| anzeigen (Benutzerdetails) | **v** (view) |
| ändern (Benutzerbeschreibung) | **m** (modify) |
| Konto gültig | **m** (modify) |
| Kennwort zurücksetzen | **W** (password) |
| Kennwort gültig | **W** (password) |

Diese Operationen können Sie mit den entsprechenden Befehlen des Dienstprogramms **pdadmin** ausführen.

### Anmerkungen:

- Mit der Berechtigung create (N) in der Gruppen-ACL oder Gruppencontainer-ACL können Sie einen Benutzer erstellen oder importieren und diesen Benutzer in die von Ihnen gesteuerte Gruppe einfügen.

  ```
  user create user1 "cn=user1,c=us" user1 user1 adcde group1

  user import user2 "cn=user2,c=us" group1
  ```

- Sie können einen Benutzer auch ohne Angabe einer Gruppe erstellen. In diesem Fall muss sich die Berechtigung create (N) jedoch in einer Zugriffssteuerungsliste (ACL) im Containerobjekt /Management/Users befinden.

  Die /Management/Users zugeordnete ACL definiert die Berechtigungen für alle Benutzer (unabhängig davon, ob sie zu einer Gruppe gehören oder nicht).

- Ein Gruppenadministrator kann eine Operation für einen Benutzer ausführen, wenn er über die entsprechende Berechtigung verfügt, die in einer der Gruppen, zu denen dieser Benutzer gehört, definiert ist.
- Gehört ein Benutzer keiner Gruppe an, muss ein Administrator über entsprechende Berechtigungen in einer ACL für /Management/Users verfügen, um Operationen für diesen Benutzer ausführen zu können.
- Die Berechtigung password (W) ist geeignet für Help-Desk-Bediener, die Benutzer mit verloren gegangenen Kennwörtern unterstützen müssen.

  Der Bediener kann das verlorene Kennwort auf einen bekannten Wert zurücksetzen und dann für **user modify password-valid** (**pdadmin**) "no" definieren. Hierdurch ist der Benutzer gezwungen, das Kennwort bei der nächsten Anmeldung zu ändern.
- Mit der Berechtigung view (v) wird die Ausgabe der Befehle **user list**, **user list-dn**, **user show groups**, **group list** und **group list-dn** gesteuert. Die Berechtigung view filtert die Ausgabe dieser Befehle. Verfügt der Benutzer nicht über die Berechtigung view für eine Gruppe oder einen Benutzer, die bzw. den der Befehl zurückgibt, wird diese Gruppe bzw. dieser Benutzer aus der Ausgabe herausgefiltert.

## Stellvertreterverwaltungs-Policy verwalten

In den beiden vorangegangenen Abschnitten wurde das Delegieren der Verwaltung der Sicherheits-Policy zum Schutz der Ressourcen in Ihrer gesicherten Domäne und das Delegieren der Verwaltung der Benutzer, die auf diese Ressourcen zugreifen, getrennt voneinander beschrieben. Diese beiden Einzelaspekte der Stellvertreterverwaltung müssen häufig kombiniert werden, um eine vollständige Sicherheits-Policy für die Stellvertreterverwaltung einzurichten.

Hierbei müssen Sie jedoch sehr vorsichtig vorgehen. Insbesondere müssen Sie genau darauf achten, welche Berechtigungskombinationen Sie erteilen.

Die Berechtigung “A” sollte beispielsweise nur den mächtigsten und sichersten Administratoren (und vielleicht auch überhaupt nicht) in Verbindung mit der Berechtigung “m” oder “W” erteilt werden. Wenn ein Administrator über die Berechtigungen “A” und “W” verfügt, kann er der Gruppe, für die er über die genannten Berechtigungen verfügt, einen beliebigen Benutzer hinzufügen und dann das Kennwort dieses Benutzers ändern. Ein beliebiger Benutzer kann ausgewählt werden, selbst ein übergeordneter Administrator oder sogar **sec_master**. Auf diese Weise könnte ein Administrator uneingeschränkten Zugriff auf das System erhalten, indem er sich als dieser übergeordnete Benutzer anmeldet. Eine Kombination der Berechtigungen “A” und “m” hat ähnliche Konsequenzen. Allerdings kann ein Administrator mit diesen beiden Berechtigungen nur beliebige Konten inaktivieren.

Bei der Definition einer vollständigen Stellvertreterverwaltungs-Policy implizieren diese Einschränkungen eine bestimmte Struktur und Verwendung für Ihre Benutzergruppen.

Sie müssen Gruppen erstellen, mit denen Sie Benutzerverwaltungs-Tasks delegieren — z. B. das Erstellen neuer Benutzer, das Löschen von Benutzern und das Zurücksetzen von Benutzerkennwörtern. Administratoren, die Benutzerverwaltungs-Tasks ausführen, sollten über die Berechtigungen “N”, “d”, “m”, “W” und “v” verfügen, um erstellen, löschen, ändern (inaktivieren oder Beschreibung ändern) zu könnnen, Kennwörter zurücksetzen oder ungültig machen zu können und um Benutzer anzeigen zu können, für deren Verwaltung sie zuständig sind. Diese Gruppen werden nur zum Delegieren der Benutzerverwaltung verwendet und sollten nicht zum Schutz anderer Ressourcen in der gesicherten Domäne verwendet werden. Außerdem müssen Sie Gruppen erstellen, mit denen Sie die Verwaltung der Sicherheits-Policy für geschützte Ressourcen in der gesicherten Domäne delegieren. Administratoren, die die Sicherheits-Policy für diese Gruppen steuern, sollten über die Berechtigungen “A” und “v”, aber nicht über die Berechtigung “N”, “d”, “m” oder “W” verfügen. Mit Hilfe dieser Gruppen wird der Zugriff auf die echten Ressourcen, die geschützt werden müssen, gesteuert.

**Beispiel:**

Sie haben einen Webbereich, auf den über das Internet zugegriffen werden kann, mit Ressourcen, die:

- allgemein zugänglich sein sollten
- nur für Kunden und Mitarbeiter zugänglich sein sollten
- nur für Mitarbeiter zugänglich sein sollten

Der Bereich kann wie folgt strukturiert werden:

```
/WebSEAL/
     www.company_xyz.com/
          customers/
          sales/
```

Eine Zugriffssteuerungsliste (ACL) am Stamm (Root) des Webbereichs von www.company_xyz.com gestattet öffentliche Zugriffsberechtigung auf den gesamten Webbereich. Eine ACL für **customers** gestattet den Zugriff durch Kunden und Vertriebsmitarbeiter, und eine weitere ACL für **sales** gestattet den Zugriff ausschließlich durch Vertriebsmitarbeiter. Diese ACLs könnten wie folgt aussehen:

```
öffentliche Zugriffsberechtigung
    Benutzer sec_master  -abc---Tdm----lrx
    Beliebige andere     -------T------lrx
    Nicht authentifiziert-------T------lrx
Kundenzugriffsberechtigung
    Benutzer sec_master  -abc---Tdm----lrx
    Gruppe customers     -------T------lrx
    Gruppe sales         -------T------lrx
    Beliebige andere     -----------------
    Nicht authentifiziert-----------------
Vertriebszugriffsberechtigung
    Benutzer sec_master  -abc---Tdm----lrx
    Gruppe sales         -------T------lrx
    Beliebige andere     -----------------
    Nicht authentifiziert-----------------
```

Diese ACLs würden jeweils wie folgt zugeordnet:

```
/WebSEAL/www.compan_xyz.com
/WebSEAL/www.company_xyz.com/customers
/WebSEAL/www.company_xyz.com/sales
```

Beispiel: Sie verfügen über die folgende Stellvertreterbenutzerverwaltungs-Policy: Vertriebsmitarbeiter (Mitglieder der Gruppe “sales”) können neue Konten für Kunden erstellen und ihnen eine Zugriffsberechtigung für den Abschnitt **customers** des Webbereichs erteilen. Nur Administratoren (Mitglieder der Gruppe “sales-admin”) können Konten für neue Vertriebsmitarbeiter verwalten.

Diese Policy wird durch folgende Gruppenstruktur implementiert:

```
/Management/
   Groups/
       sales            <- ACL sales-admin
       sales-users      <- ACL sales-users-admin
       customers        <- ACL customers-admin
       customers-users  <- ACL customers-users-admin
```

Die ACL **sales-admin** dient zur Verwaltung der Zugehörigkeit zur Gruppe ’sales’, die wiederum den Zugriff auf den Abschnitt des Webbereichs steuert, der den Vertriebsmitarbeitern vorbehalten ist. Nur die Berechtigung der Gruppe “sales-admin” zum Hinzufügen und Entfernen von Benutzern in dieser Gruppe ist erforderlich. Außerdem ist die Berechtigung view (v) nützlich für Administratoren, damit sie die Gruppenzugehörigkeit und die Benutzer in der Gruppe anzeigen können.

```
sales-admin
    Gruppe super-admin  Tabc
    Gruppe admin        TAv
```

Die ACL **sales-users-admin** steuert durch die Zuordnung zur Gruppe **sales-users**, wer Benutzer verwalten kann, die zur Gruppe **sales-users** gehören (das ist wieder die Gruppe “sales-admin”).

```
sales-users-admin
    Gruppe super-admin  Tabc
    Gruppe admin        TNWdmv
```

Ähnlich dient die ACL **customers-admin** zur Verwaltung der Zugehörigkeit zur Gruppe **customers**, die wiederum den Zugriff auf den Abschnitt des Webbereichs steuert, der den Kunden vorbehalten ist.

```
customers-admin
    Gruppe super-admin  Tabc
    Gruppe sales        TAv
```

Die ACL **customers-users-admin** steuert durch die Zuordnung zur Gruppe **customers-users**, wer die Mitglieder der Gruppe **customers-users** verwalten kann (das ist wieder die Gruppe ’sales’). Auch die Mitglieder der Gruppe “sales-admin” dürfen Kunden verwalten.

```
customers-users-admin
    Gruppe super-admin   Tabc
    Gruppe group sales   TNWdmv
    Gruppe admin         TNWdmv
```

Beachten Sie, dass in jeder ACL einer Gruppe **super-admin** die Berechtigung zum Hinzufügen, Durchsuchen und Steuern erteilt wird. Die Mitglieder der Gruppe **super-admin** sind verantwortlich für die Verwaltung dieser ACLs.



# Policy Director-Server verwalten

Dieses Kapitel enthält ausführliche Informationen zur Ausführung allgemeiner Verwaltungs- und Konfigurations-Tasks auf den Policy Director-Servern. Außerdem enthält es Erläuterungen zu den Konfigurationsdateien, die die einzelnen Server unterstützen.

Stichwortindex:



## Policy Director-Server - Einführung

Policy Director besteht aus folgenden Serverprozessen (Dämonen):

- Management Server (**pdmgrd**)
- Authorization Server (**pdacld**)
- WebSEAL (**webseald**)

Diese Server werden während der Produktinstallation automatisch konfiguriert und aktiviert.

Der Management Server (**pdmgrd**) verwaltet die Hauptberechtigungsdatenbank (ACL) und Adressinformationen zu anderen Policy Director-Servern in einer gesicherten Domäne. Der Management Server erfordert normalerweise sehr wenig Verwaltung oder Konfiguration.

Der Authorization Server (**pdacld**) gestattet Anwendungen anderer Hersteller, Berechtigungsaufrufe (über die Berechtigungs-API) an den Policy Director-Sicherheitsservice durchzuführen. Der Authorization Server erfordert normalerweise sehr wenig Verwaltung oder Konfiguration.

WebSEAL (**websealD**) ist ein Webserver mit hoher Leistung und mehreren Threads, der eine feinkörnige Sicherheits-Policy auf den geschützten Webobjektbereich anwendet. WebSEAL kann Lösungen mit Einzelanmeldung zur Verfügung stellen und Backend-Webanwendungsserverressourcen in seine Sicherheits-Policy integrieren.

## Serverabhängigkeiten

Wichtige Abhängigkeiten des Policy Director-Servers:

- Eine gesicherte Domäne darf nur ein Exemplar des Verwaltungsservers und der Hauptberechtigungsdatenbank (ACL-Datenbank) enthalten.
- Der Verwaltungsserver repliziert (vervielfältigt) die Berechtigungsdatenbank für alle anderen Policy Director-Server in der gesicherten Domäne.
- Jeder Ressourcenmanager (z. B. WebSEAL und der Authorization Server) wendet Zugriffssteuerungs-Policy auf der Grundlage von Informationen aus der Replikationsberechtigungsdatenbank an.

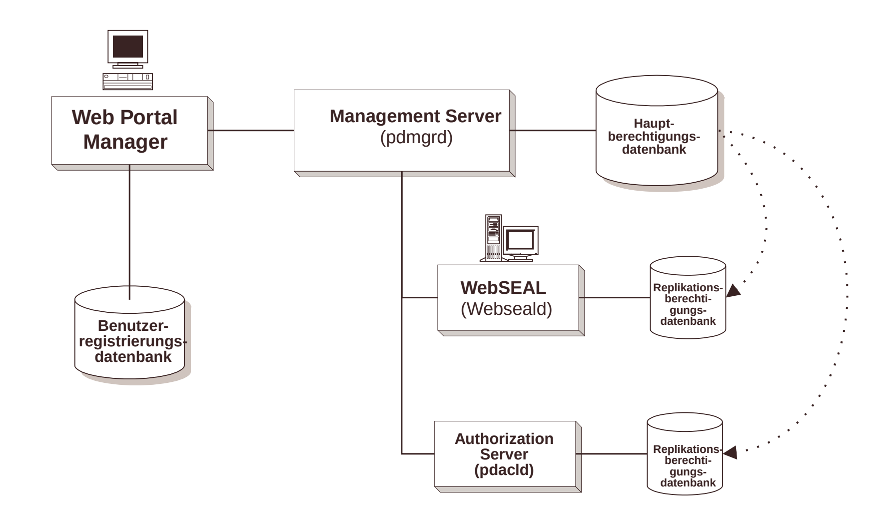



*Abbildung 28. Policy Director-Serverkomponenten*

# Einführung in Serververwaltungs-Tools

Folgende Schnittstellen stehen für bestimmte Verwaltungs-Tasks zur Verfügung:

- Web Portal Manager
- Dienstprogramm **pdadmin**
- Dienstprogramm **pd_start**
- Windows NT-Systemsteuerung ’Dienste’

Führen Sie die meisten Serververwaltungs-Tasks über die grafische Benutzerschnittstelle (Graphical User Interface, GUI) der Management Console aus. Für spezifische Tasks, die die Management Console nicht abdeckt, verwenden Sie eins der anderen Dienstprogramme.

**pdadmin** und die UNIX-Start-Scripts stellen Befehlszeilenschnittstellen zur Verfügung. Befehlszeilenausdrücke sind nützlich, wenn Serververwaltungs-Tasks innerhalb von Shell-Scripts automatisiert werden.

Web Portal Manager und **pdadmin** können sowohl fern als auch lokal verwendet werden. Die Start-Scripts müssen lokal verwaltet werden.

Bei der Fehlerbehebung können die Befehlszeilendienstprogramme Statusinformationen und Steuerung einzelner Server zur Verfügung stellen.

## Web Portal Manager

- Siehe *Tivoli SecureWay Policy Director Web Portal Manager for Windows Administratorhandbuch*.

## Dienstprogramm pdadmin

Policy Director stellt das Befehlszeilendienstprogramm **pdadmin** für die meisten Server-Tasks zur Verfügung. Mit **pdadmin** können Sie folgendes ausführen:

- Alle Verwaltungs-Tasks, die über die Management Console zur Verfügung stehen, ausführen
- Alle Verwaltungs-Tasks, die nicht über die Management Console zur Verfügung stehen, ausführen
- Siehe „Referenz für Befehl pdadmin” auf Seite 197

### Dienstprogramm pd_start

Administratoren können mit Hilfe des Dienstprogramms **pd_start** Server manuell stoppen, starten, erneut starten und den Serverstatus anzeigen.

### Systemsteuerung für Windows NT-Dienste

Über die Systemsteuerung für Dienste können Sie folgendes ausführen:

- Server stoppen
- Server starten
- Server anhalten (aussetzen)
- Angehaltenen Server fortsetzen (wieder aufnehmen)
- Konfigurierte Server auflisten

## Serverkonfigurationsdateien

Mit Hilfe der Serverkonfigurationsdateien können Sie die Verarbeitung der Policy Director-Server anpassen:

| Servername | Konfigurations-datei | Position der Konfigurationsdatei |
|---|---|---|
| **Management Server** (pdmgrd) | ivmgrd.conf | **UNIX:** <*Installationspfad*>/etc/ivmgrd.conf<br>**Windows:** <*Installationspfad*>\etc\ivmgrd.conf |
| **Authorization Server** (pdacld) | ivacld.conf | **UNIX:** <*Installationspfad*>/etc/ivacld.conf<br>**Windows:** <*Installationspfad*>\etc\ivacld.conf |
| **WebSEAL** (webseald) | webseald.conf | **UNIX:** /opt/pdweb/etc/webseald.conf<br>**Windows:** C:\Programme\Tivoli\PDWeb\etc\webseald.conf |

Die Policy Director Base-Programmdateien werden in folgendem Stammverzeichnis installiert:

UNIX: `/opt/PolicyDirector/`
Windows: `C:\Programme\Tivoli\Policy Director\`

In diesem Handbuch wird dieses Stammverzeichnis durch die Variable **<Installationspfad>** dargestellt. Alle relativen Pfadnamen, die in den Policy Director-Konfigurationsdateien angegeben sind, beziehen sich auf dieses Stammverzeichnis. Konfigurationsdateien sind textbasierte ASCII-Dateien, die mit Hilfe eines allgemeinen Texteditors bearbeitet werden können. Die Konfigurationsdateien enthalten Parametereinträge in folgendem Format:

```
Parameter=Wert
```

Bei der Erstinstallation von Policy Director werden Standardwerte für die meisten Parameter festgelegt. Einige Parameter sind statisch und ändern sich nie. Andere können der Serverfunktionalität und -leistung entsprechend geändert werden.

**Anmerkung:** Nach dem Editieren einer Konfigurationsdatei müssen Sie den Policy Director-Server stoppen und erneut starten, damit die Änderungen wirksam werden.

Jede Datei enthält Abschnitte, so genannte **Zeilengruppen**, die mindestens einen Parameter für eine bestimmte Konfigurationskategorie enthalten. Die Zeilengruppenbezeichnungen stehen zwischen eckigen Klammern: [*Zeilengruppenname*].

Die Zeilengruppe **[ssl]** in `ivmgrd.conf` definiert beispielsweise die SSL-Konfigurationseinstellungen für den Management Server. Die Zeilengruppe **[ldap]** definiert die vom Management Server benötigte Konfiguration für die Kommunikation mit dem LDAP-Registrierungsdatenbankserver. Die Dateien enthalten Kommentare, die die Verwendung der einzelnen Parameter erläutern.

Wenn Sie Konfigurationseinstellungen ändern müssen, gehen Sie beim Editieren der Dateien mit Vorsicht vor, um ihre Integrität sicherzustellen.

# UNIX: Policy Director-Server stoppen/starten

Serverprozesse werden normalerweise durch automatisierte Scripts, die beim Systemstart und beim Systemabschluss ausgeführt werden, aktiviert bzw. inaktiviert.

In einer UNIX-Umgebung können Sie mit dem Script **pd_start** die Serverprozesse auch manuell starten und stoppen. Dieses Verfahren ist nützlich, wenn Sie eine Installation anpassen oder Fehlerbehebungs-Tasks ausführen müssen. Scripts können Sie nur auf der lokalen Maschine ausführen. Für das ferne Stoppen und Starten von Servern verwenden Sie Web Portal Manager.

Die allgemeine Syntax für **pd_start** lautet:

```
# pd_start {start|restart|stop|status}
```

Sie können das Dienstprogramm **pd_start** aus jedem Verzeichnis ausführen. Das Script befindet sich in folgendem Verzeichnis:

```
/opt/PolicyDirector/bin/
```

## Policy Director-Server mit Dienstprogramm pd_start stoppen

Verwenden Sie das Dienstprogramm **pd_start**, um alle Policy Director-Server auf einer bestimmten Maschine in der korrekten Reihenfolge zu stoppen:

```
# pd_start stop
```

Dieses Script wartet, bis alle Server gestoppt wurden, bevor die Eingabeaufforderung wieder erscheint.

## Policy Director-Server mit Dienstprogramm pd_start starten

Verwenden Sie das Dienstprogramm **pd_start**, um alle Policy Director-Server, die auf einer bestimmten Maschine momentan nicht aktiv sind, zu starten.

```
# pd_start start
```

Dieses Script wartet, bis alle Server gestartet wurden, bevor die Eingabeaufforderung wieder erscheint.

## Policy Director-Server mit Dienstprogramm pd_start erneut starten

Verwenden Sie das Dienstprogramm **pd_start**, um alle Policy Director-Server auf einer bestimmten Maschine zu stoppen und dann erneut zu starten:

```
# pd_start restart
```

Dieses Script wartet, bis alle Server gestartet wurden, bevor die Eingabeaufforderung wieder erscheint.

## Einzelne Server manuell starten

Sie können die Server einzeln manuell starten, indem Sie die Server direkt ausführen. Der Server initialisiert sich selbst und, falls erfolgreich, startet die Dämonen selbst.

Sie müssen die Startbefehle als Verwaltungsbenutzer, z. B. **root**, ausführen.

Starten Sie die Policy Director-Server in folgender Reihenfolge:

1. Management Server (**pdmgrd**):

   ```
   # <Installationspfad>/bin/pdmgrd
   ```

2. Authorization Server (**pdacld**):

   ```
   # <Installationspfad>/bin/pdacld
   ```

## Serverstatus mit Dienstprogramm pd_start anzeigen

Mit dem Befehl **pd_start** können Sie den Serverstatus anzeigen:

```
# pd_start status
Policy Director-Server:
Server       Aktiviert      Aktiv
pdmgrd        ja             ja
webseald      nein           nein
pdacld        ja             nein
```

# Windows: Policy Director-Server stoppen/starten

Über die Systemsteuerung für Windows NT-Dienste können Sie die Serverprozesse manuell starten und stoppen. Dies kann bei der Anpassung einer Installation oder bei der Fehlerbehebung nützlich sein. Für die Verwendung dieses Dienstprogramms sind Verwaltungsberechtigungen erforderlich.

Sie können alle Policy Director-Server auf einmal oder einzeln starten und stoppen. Die Server müssen in der Regel in der korrekten Reihenfolge gestoppt und gestartet werden.

## Server über Systemsteuerung - Dienste stoppen/starten

Der **Autostart-Dienst** startet die Policy Director-Server, wenn in der Konfiguration für die **Startart** "Automatisch" angegeben ist. Sobald der Server startet, wird der Autostart-Dienst beendet.

Sie können über Systemsteuerung -> Dienste die einzelnen Server auch manuell starten und stoppen:

1. Öffnen Sie die Windows-Systemsteuerung.
2. Klicken Sie das Symbol 'Dienste' doppelt an.

   Das Dialogfenster 'Dienste' wird angezeigt.
3. Wählen Sie die Policy Director-Server in der Reihenfolge, die in Schritt 4 und 5 angegeben ist, aus dem Listenfenster aus.
4. **Stoppen** Sie die Policy Director-Server in folgender Reihenfolge:
   - Berechtigungsserver
   - Verwaltungsserver
5. **Starten** Sie die Policy Director-Server in folgender Reihenfolge:
   - Verwaltungsserver
   - Berechtigungsserver

6. Klicken Sie den entsprechenden Knopf (Starten, Beenden, Startart) auf der rechten Seite des Fensters.
7. Damit ein Policy Director-Server nicht automatisch durch den Dienst ’Autostart’ gestartet wird, drücken Sie den Knopf “Startart...”, um für diesen Server ’Deaktiviert’ anzugeben.

# Serverstart beim Systemstart automatisieren

Parameter zum Automatisieren des Serverstarts befinden sich in der Zeilengruppe **[pdrte]** der Konfigurationsdatei `pd.conf`.

## Management Server

Wenn das Paket **PDMgr** installiert ist, startet der Management Server-Dämon (**pdmgrd**) automatisch nach jedem Neustart des Systems:

```
[pdrte]
boot-start-ivmgrd = yes
```

Soll der automatische Start von **pdmgrd** verhindert werden, geben Sie folgendes an:

```
boot-start-ivmgrd = no
```

**Anmerkung:** Jede gesicherte Domäne darf nur einen Management Server enthalten. **pdmgrd** darf nicht auf mehreren Servern pro gesicherter Domäne installiert und ausgeführt werden.

## Authorization Server

Wenn das Paket **PDAcld** installiert ist, startet der Authorization Server-Dämon automatisch nach jedem Neustart des Systems:

```
[pdrte]
boot-start-ivacld = yes
```

Soll der automatische Start von **pdacld** verhindert werden, geben Sie folgendes an:

```
boot-start-ivacld = no
```

# Verwaltung des Management Servers (pdmgrd)

Der Management Server verwaltet die Hauptberechtigungs-Policy-Datenbank und Adressinformationen zu anderen Policy Director-Servern in der gesicherten Domäne. Der Management Server erfordert normalerweise sehr wenig Verwaltung oder Konfiguration. Dieser Abschnitt beschreibt die Konfigurations-Tasks, die dem Administrator zur Verfügung stehen.


- „Replikation der Berechtigungsdatenbank” auf Seite 145
- „Anzahl der Aktualisierungsbenachrichtigungs-Threads definieren” auf Seite 147
- „Benachrichtigungsverzögerungszeit definieren” auf Seite 148


## Replikation der Berechtigungsdatenbank

Ein Policy Director-Administrator kann jederzeit Änderungen der Sicherheits-Policy in der gesicherten Domäne vornehmen. Eine Hauptaufgabe des Management Servers besteht in der erforderlichen, diesen Änderungen entsprechenden Anpassung der Hauptberechtigungsdatenbank.

Wenn der Management Server eine Änderung in der Hauptberechtigungsdatenbank vornimmt, kann er einen Hinweis auf diese Änderung an alle Authorization Server (mit Replikationsdatenbanken) senden. Die Authorization Server müssen dann eine Datenbankaktualisierung von der Hauptberechtigungsdatenbank anfordern.

**Anmerkung:** Außerdem können Client-Server Datenbankaktualisierungen durch regelmäßige Sendeaufrufe an den Management Server prüfen. Die Konfiguration des Sendeaufrufs für einen WebSEAL-Client wird z. B. im *Tivoli SecureWay Policy Director WebSEAL Administratorhandbuch* erläutert.

Mit Hilfe von Policy Director können Sie Aktualisierungsbenachrichtigungen vom Management Server als automatischen Prozess oder als manuell gesteuerte Task konfigurieren. Der Parameter **auto-database-update-notify** befindet sich in der Zeilengruppe **[ivmgrd]** der

Konfigurationsdatei `ivmgrd.conf`. Für den Parameter ist standardmäßig “yes” definiert (der Management Server führt die Aktualisierungsbenachrichtigung automatisch durch):

```
[ivmgrd]
auto-database-update-notify = yes
```

Diese automatische Einstellung ist für Umgebungen geeignet, in der Datenbankänderungen selten vorkommen. Wenn Sie eine automatische Aktualisierungsbenachrichtigung konfigurieren, müssen Sie auch die Parameter **max-notifier-threads** und **notifier-wait-time** korrekt konfigurieren. Siehe „Anzahl der Aktualisierungsbenachrichtigungs-Threads definieren” auf Seite 147 and „Benachrichtigungsverzögerungszeit definieren” auf Seite 148.

Wenn Sie eine manuelle Aktualisierungsbenachrichtigung konfigurieren, wird dieses Ereignis durch eine manuelle Anwendung des Befehls **pdadmin server replicate** gesteuert.

```
[ivmgrd]
auto-database-update-notify = no
```

Diese manuelle Einstellung ist für Umgebungen geeignet, in der Datenbankänderungen häufig vorkommen und tiefgreifende Änderungen nach sich ziehen. In einigen Fällen können einige Datenbankänderungen viele Aktualisierungsbenachrichtigungen generieren, die bald veralten, weil die Hauptdatenbank fortlaufend geändert wird. Diese veralteten Benachrichtigungen verursachen unnötigen Datenaustausch auf dem Netz.

Durch eine manuelle Steuerung der Aktualisierungsbenachrichtigungen kann die Änderung der Hauptberechtigungsdatenbank abgeschlossen werden, bevor Aktualisierungsbenachrichtigungen an Authorization Server mit Datenbankreplikationen gesendet werden.

Im manuellen Modus wird für die Aktualisierungsbenachrichtigung der Benachrichtigungs-Thread-Pool verwendet (wie auch im automatischen Modus). Daher wirkt sich die Einstellung des Parameters **max-notifier-threads** auf den manuellen Modus aus. Siehe „Anzahl der Aktualisierungsbenachrichtigungs-Threads definieren” auf Seite 147.

### Befehl pdadmin server replicate

Wenn Sie eine manuelle Aktualisierungsbenachrichtigung konfigurieren, wird dieses Ereignis durch eine manuelle Anwendung des Befehls **pdadmin server replicate** gesteuert. Der Befehl hat folgende Syntax:

```
pdadmin> server replicate [-server <Servername>]
```

Wird das optionale Argument **Servername** angegeben, wird nur dieser Server über Änderungen der Hauptberechtigungsdatenbank informiert. In einer Antwort wird der Erfolg bzw. Misserfolg der Benachrichtigung und der Replikation angezeigt.

Wird das Argument **Servername** nicht angegeben, empfangen alle konfigurierten Authorization Server Aktualisierungsbenachrichtigungen. Eine positive Antwort zeigt lediglich an, dass der Management Server mit dem Senden von Aktualisierungsbenachrichtigungen begonnen hat. Die Antwort gibt keine Auskunft darüber, ob die eigentlichen Benachrichtigungs- und Replikationsprozesse erfolgreich waren oder nicht.

Für die Ausführung dieses Befehls ist die Berechtigung “s” für das Objekt /Management/Server erforderlich.

## Anzahl der Aktualisierungsbenachrichtigungs-Threads definieren

Der Verwaltungsserver ist für das Synchronisieren aller Datenbankreplikationen in der gesicherten Domäne verantwortlich. Wenn in der Hauptdatenbank eine Änderung vorgenommen wird, übernehmen Benachrichtigungs-Threads das Melden dieser Änderung an alle Replikationen. Jede Replikation ist dann dafür zuständig, die neuen Informationen aus der Hauptdatenbank herunterzuladen.

Die Konfigurationsdatei des Verwaltungsservers, `ivmgrd.conf`, enthält einen Parameter, mit dem die maximale Anzahl der Aktualisierungsbenachrichtigungs-Threads definiert werden kann.Dieser Thread-Pool gestattet simultane (parallele) Benachrichtigung.

Sollen beispielsweise 30 Replikationen über eine Datenbankänderung informiert werden, muss für den Thread-Pool mindestens 30 angegeben werden. Sind mehr als 30 Replikationen vorhanden, erfolgt die Benachrichtigung der übrigen Replikationen in einem neuen Durchgang (in diesem Beispiel jeweils 30 gleichzeitig). Alle Replikationen werden benachrichtigt, unabhängig von dem Wert dieses Parameters.

Das Ziel des Aktualisierungsbenachrichtigungs-Thread-Werts ist die schnellstmögliche Bekanntgabe einer Datenbankänderung. Der Wert sollte normalerweise der Anzahl der vorhandenen Replikationen entsprechen. Auf diese Weise ist eine bessere Leistung zu erwarten, da ein einzelner Thread-Pool die Benachrichtigung aller Replikationen auf einmal schneller durchführen kann.

Der Standardwert für den Ereignisbenachrichtigungs-Thread-Pool lautet:

```
[ivmgrd]
max-notifier-threads = 10
```

Siehe auch „Benachrichtigungsverzögerungszeit definieren".

## Benachrichtigungsverzögerungszeit definieren

Wenn der Verwaltungsserver eine Anweisung für eine Änderung der Hauptberechtigungsdatenbank erhält, verzögert er das Senden der Benachrichtigungen an Datenbankreplikationen über einen Standardzeitraum. Die Standardverzögerungszeit ist auf 15 Sekunden festgelegt. Diese Zeitverzögerung wird mit jeder nachfolgenden Änderung der Datenbank zurückgesetzt.

Die zeitliche Verzögerung soll verhindern, dass der Verwaltungsserver einzelne Replikationsbenachrichtigungen für jede Änderung in einer Reihe von Datenbankänderungen sendet. Die zeitliche Verzögerung unterstützt die Gewährleistung einer optimalen Leistung des Policy Director-Systems.

Diese Funktion ist besonders wichtig in Umgebungen, in denen Stapelverarbeitungsänderungen in der Berechtigungsdatenbank vorgenommen werden. Hierbei ist es effektiver, Policy-Änderungen erst dann an Datenbankreplikationen zu senden, wenn alle Änderungen abgeschlossen sind.

Sie können diesen Standardwert der Benachrichtigungszeitverzögerung überschreiben, indem Sie den Wert des Parameters **notifier-wait-time** (in Sekunden) ändern. Dieser Parameter befindet sich in der Zeilengruppe **[ivmgrd]** der Konfigurationsdatei `ivmgrd.conf`. Zum Beispiel:

```
[ivmgrd]
notifier-wait-time = 20
```

Der Standardwert ist 15 Sekunden.



# LDAP-Registrierungsdatenbank verwenden

LDAP ist ein Protokoll, das über TCP/IP ausgeführt wird. Der LDAP-Protokollstandard beinhaltet einfache Netzprotokolldefinitionen sowie Datendarstellungs- und -bearbeitungsfunktionen.

Ein Verzeichnis, auf das über LDAP zugegriffen werden kann, wird üblicherweise als LDAP-Verzeichnis bezeichnet.

Die Standardinstallation von Policy Director verwendet ein LDAP-Verzeichnis zum Speichern von Benutzerinformationen. Die IBM Implementierung von LDAP wird als IBM SecureWay Directory bezeichnet. Die iPlanet-Implementierung von LDAP wird als iPlanet Directory Server bezeichnet. Dieses Kapitel erläutert Konfigurationsmerkmale der Policy Director-LDAP-Registrierungsdatenbank.

Stichwortindex:

# LDAP-Übersicht

Im Jahr 1988 entwickelte das CCITT (Comite Consultatif International Telephonique et Telegraphique, das jetzt ITU-T, International Telecommunications Union -Telecommunication Standardization Sector, heißt) einen Standard für Verzeichnisservices mit dem Namen X.500. Der X.500-Verzeichnisservice wurde im Jahr 1990 zu ISO Standard 9594 (Data Communications Network Directory, Recommendations X.500-X.521).

Die ISO-Standardgruppe wird weiterhin üblicherweise als X.500 bezeichnet. X.500 definiert ein Verzeichnis, das universell für große Datenmengen verwendet werden kann. Heute werden X.500-Verzeichnisse von nationalen Telefongesellschaften für große Onlinetelefonverzeichnisse verwendet.

Für den Zugriff auf ein X.500-Verzeichnis verwendet ein Client das Directory Access Protocol (DAP), das in Verbindung mit dem X.500-Standard definiert wurde. Leider ist DAP ein sehr komplexes Protokoll, das auf kleinen Clients, z. B. Desktop-Computer, nicht ohne weiteres unterstützt werden kann.

X.500 war daher auf leistungsfähige Computer und große Implementierungen beschränkt. Die Notwendigkeit, auf zentrale Verzeichnisse von kleinen Clients aus zuzugreifen, wurde jedoch für die Unterstützung der offensichtlichen Kostenwirksamkeit zentraler Verzeichnisse wichtig.

Aufgrund von Arbeiten an der University of Michigan und in der Netscape Communications Corporation wurde eine vereinfachte Version von DAP entwickelt, die den Namen Lightweight Directory Access Protocol (LDAP) trägt. LDAP unterstützt die meisten Funktionen von DAP; einige der komplexen und selten verwendeten Funktionen fehlen jedoch. Die LDAP-Implementierung ist relativ einfach und kann von Desktop-Anwendungen verwendet werden.

## LDAP: Ein Protokoll für Verzeichnisservices

LDAP ist ein Protokoll, das über TCP/IP ausgeführt wird. Der LDAP-Protokollstandard beinhaltet einfache Netzprotokolldefinitionen sowie Datendarstellungs- und -bearbeitungsfunktionen.

Ein Verzeichnis, auf das über LDAP zugegriffen werden kann, wird üblicherweise als LDAP-Verzeichnis bezeichnet.

**Anmerkung:** Der LDAP-Standard definiert nicht, wie die Daten in dem Verzeichnis gespeichert werden.

Zunächst war LDAP so angelegt, dass kleine Clients über einen Gateway-Server, der die Umsetzung zwischen LDAP und DAP durchführte, auf ein X.500-Verzeichnis zugreifen konnten.

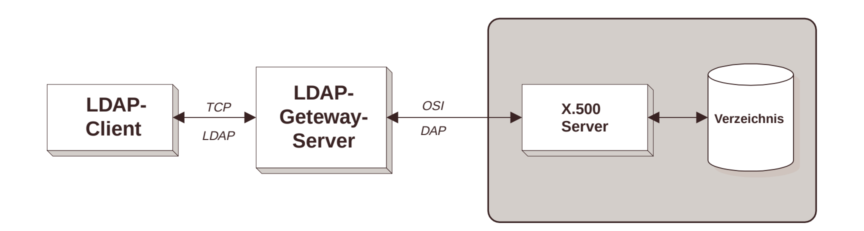



*Abbildung 29. LDAP-Zugriff auf X.500*

Bald wurden Verzeichnisse entwickelt, die das LDAP-Protokoll nativ ohne eine Umsetzung zwischen LDAP und DAP handhaben konnten.

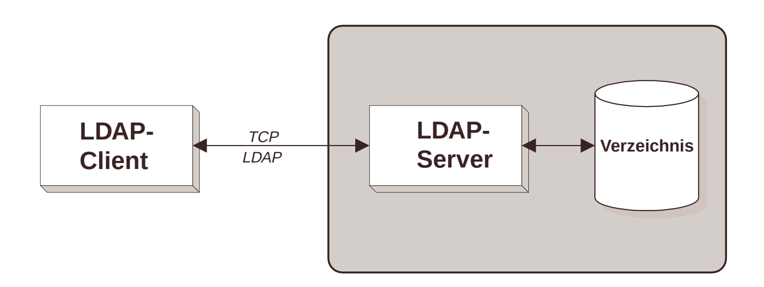



*Abbildung 30. Standalone-LDAP-Server*

Die IBM Implementierung eines LDAP-Verzeichnisses ist SecureWay Directory, das unter AIX, Windows NT, Sun Solaris, OS/400 und OS/390 zur Verfügung steht.

Ein LDAP-Verzeichnis kann eine beliebige Speicherimplementierung für die Verzeichnisdaten verwenden. Die meisten Implementierungen verwenden zwar Flachdateidatenbanken, IBM SecureWay Directory verwendet jedoch die relationale DB2-Hochleistungsdatenbank als Speicherimplementierung.

## LDAP-Verzeichnisse

In den meisten Verzeichnissen werden Informationen mit einer ähnlichen Struktur wie in einem gedruckten Telefonbuch gespeichert. Die Einträge sind in der Regel hierarchisch angeordnet, was effizientes und flexibles Verwalten und Suchen gestattet.

LDAP-Verzeichnisse sind sehr viel leistungsfähiger; sie sind nicht auf Namen, Rufnummer und Adresseinträge beschränkt. In einem LDAP-Verzeichnis können fast alle Datenarten gespeichert (und folglich auch abgerufen) werden. Der Datentyp, der in einem LDAP-Verzeichnis gespeichert werden kann, wird durch das Verzeichnisschema definiert, das Ihren Anforderungen entsprechend erweitert und angepasst werden kann.

Das Definieren eines Verzeichnisschemas und der hierarchischen Verzeichnisinformationsbaumstruktur kann mit dem Aufbau einer relationalen Datenbank verglichen werden. Für den Entwurf eines Verzeichnisschemas und einer Verzeichnisinformationsbaumstruktur (Directory Information Tree, DIT) ist gründliche Analyse der Anwendungsvoraussetzungen, der Unternehmensstandards und der Datendefinitionen erforderlich.

LDAP-Serverprodukte, z. B. IBM SecureWay Directory, stellen ein umfassendes Schema zur Verfügung, das verwendet werden kann, sofern keine spezifischen Änderungen durch Anforderungen erforderlich sind.

IBM unterstützt aktuelle und in der Entwicklung befindliche Standards und Vorschläge für Datendefinitionen durch aktive Teilnahme am Standardisierungsprozess und durch Implementieren der Ergebnisse in IBM SecureWay Directory. Das wichtigste Standardisierungsorgan für LDAP ist die Internet Engineering Task Force (IETF),

in der Vertreter von IBM und andere wichtige industrielle Führungskräfte diese Aktivitäten aktiv unterstützen.

Jede Organisation verwendet Verzeichnisse. Die meisten modernen Betriebssysteme, z. B. UNIX oder Windows 9x/NT, speichern z. B. Benutzerkontodaten entweder lokal oder auf Abteilungsservern. Netzbetriebssysteme, z. B. NetWare (Novell), benötigen ebenfalls Datenbanken. Abteilungen können eine lokale Mitarbeiterdatenbank verwalten, während sich auf Unternehmensebene umfangreiche Personaldatenbanken befinden. Außerdem speichern Betriebssysteme große Datenmengen für die Systemkonfiguration und andere Netzressourcen, z. B. Drucker und Server.

Informationen werden häufig über mehrere Positionen verteilt gespeichert, wodurch Verwaltung und Pflege unnötig erschwert werden. Hauptursache dafür, dass LDAP schnell so viel Interesse erregt hat, ist die Möglichkeit, ein einzelnes, auf Standards beruhendes Verzeichnis für verteilte Informationen zu erhalten.

## Das LDAP-Informationsmodell

Das LDAP-Informationsmodell beruht auf einem Teil des X.500-Informationsmodells. Die Daten in einem LDAP-Verzeichnis werden in Einträgen gespeichert, die Attribute enthalten. Attribute werden mit folgendem Format eingegeben:

```
Typ = Wert
```

Hierbei wird der Typ durch eine Objekt-ID (OID) definiert, und der Wert hat eine definierte Syntax. Attribute können über einen Wert (z. B. kann eine Person nur ein Geburtsdatum haben) oder über mehrere Werte (eine Person kann mehrere Rufnummern haben) verfügen.

Jeder Eintrag in einem LDAP-Verzeichnis hat einen eindeutigen registrierten Namen (Distinguished Name, DN). Das Verzeichnisschema definiert Regeln für DNs und welche Attribute ein Eintrag enthalten muss. Um die in Verzeichniseinträgen gespeicherten Informationen zu organisieren, werden in dem Schema Objektklassen definiert. Eine Objektklasse besteht aus verbindlichen und optionalen Attributen.

Objektklassen können von anderen Objektklassen übernommen werden, was eine einfache Erweiterungsmethode darstellt (neue Objektklassen können z. B. definiert werden, indem vorhandenen Objektklassen lediglich neue Attribute hinzugefügt werden).

## LDAP-Merkmale

### Skalierbarkeit

LDAP-Verzeichnisse sind, insbesondere, wenn sie durch eine relationale Datenbank wie IBM SecureWay Directory gesichert werden, in hohem Maß skalierbar. Große Verzeichnisse mit Millionen von Einträgen sind bei gleichzeitig exzellenter Leistung möglich.

Aufgrund der allgemeinen Standardbasis ist die einfache Aufrüstmöglichkeit auf leistungsfähigere Hardware und Software ein weiterer Skalierbarkeitsfaktor. LDAP ist von keinem bestimmten Betriebssystem und von keinem Hersteller abhängig.

### Verfügbarkeit

LDAP unterstützt Replikation und Teilung von Namensbereichen. Durch die Replikation können mehrere LDAP-Server denselben Verzeichnisinhalt speichern. Clients profitieren von diesen zusätzlichen Servern, die zur Verfügung stehen, wenn einer ausfällt.

Durch die Teilung können Abschnitte des gesamten Verzeichnisses auf verschiedenen Servern an unterschiedlichen Positionen gespeichert werden. Hierdurch wird nicht nur die Verfügbarkeit verbessert (kein Single Point of Failure), sondern auch die verteilte Verwaltung erleichtert.

### Sicherheit

LDAP unterstützt Sicherheitseinrichtungen, die unbefugten Datenzugriff verhindern. Sichere Übertragungsprotokolle wie z. B. SSL und Authentifizierungsmethoden sowie ACL-Policies (ACL = Access Control List, Zugriffssteuerungsliste) für Dateneingaben garantieren ein Höchstmaß an Sicherheit.

### Leichte Verwaltung

Aktuelle Versionen von LDAP, z. B. IBM SecureWay Directory, stellen eine grafische Benutzerschnittstelle für die Systemverwaltung

und die Verzeichnisdatenverwaltung zur Verfügung. Dynamisch erweiterbares Schema ermöglicht eine Erweiterung des Verzeichnisschemas ohne Unterbrechung des Service.

### Standardisierung

Das LDAP-Protokoll — und viele zugehörige Client/Server-Funktionen, Anwendungsprogrammierschnittstellen (APIs) und Datendefinitionen — werden entweder durch offizielle Standards oder entsprechende RFCs (Request for Comments) definiert.

Lightweight Directory Access Protocol (v3), RFC 2251, definiert beispielsweise das LDAP-Basisprotokoll. Andere Funktionen, die allgemein akzeptiert und implementiert werden, sind in Internet-Entwürfen definiert. Ein Großteil dieser Arbeit wird durch die IETF (Internet Engineering Task Force) und die DMTF (Distributed Management Task Force) erbracht.

## LDAP-Überbrückungskonfiguration

Das Lightweight Directory Access Protocol (LDAP) definiert eine Standardmethode für den Zugriff auf und die Aktualisierung von Informationen in einem Verzeichnis. Der Zugriff auf Verzeichnisse erfolgt normalerweise mit Hilfe eines Client-/Serverübertragungsmodells. Jeder Server, der das LDAP-Protokoll implementiert, ist ein LDAP-Verzeichnisserver.

Policy Director unterstützt die Verwendung von LDAP für seine Benutzerregistrierungsdatenbank. Die IBM Implementierung von LDAP wird als IBM SecureWay Directory bezeichnet. Die iPlanet-Implementierung von LDAP wird als iPlanet Directory Server bezeichnet.

Die verteilte LDAP-Architektur unterstützt skalierbare Verzeichnisservices mit Serverreplikationsfunktionen. Die Serverreplikation verbessert die Verfügbarkeit eines Verzeichnisservice. Die IBM SecureWay Directory-Replikation basiert auf einem Master/Slave-Modell. Die iPlanet Directory Server-Replikation basiert auf einem Lieferanten-/Konsumentenmodell. Policy Director geht weiterhin von einer Master/Slave-Beziehung aus.

Die Kombination aus einem Hauptserver (Master) und mehreren Replikationsservern unterstützt die Gewährleistung, dass Verzeichnisdaten bei Bedarf immer verfügbar sind. Wenn ein Server ausfällt, ist der Verzeichnisservice weiterhin über einen anderen Replikationsserver verfügbar. Policy Director unterstützt diese Replikationsfähigkeit.

## Das Master/Slave-Replikationsmodell

Bei der Replikation gibt es zwei Verzeichnisarten: Master und Replikation (Kopie). LDAP bezeichnet den Master als Master-Server (Hauptserver) und die Replikation als Replikationsserver. Für eine bestimmte Verzeichnisstruktur gibt es einen Master-Server (den Lese-/Schreibserver). Alle Aktualisierungen werden auf dem Master-Server durchgeführt, und diese Aktualisierungen werden dann an die Replikationsserver weitergegeben. Jede Replikationsserverdatenbank enthält eine exakte Kopie der Verzeichnisdaten des Master-Servers.

Änderungen im Verzeichnis können nur auf dem Master-Server durchgeführt werden, der immer für Schreiboperationen für das Verzeichnis verwendet wird. Für Leseoperationen kann der Master-Server oder die Replikationsserver verwendet werden. Wenn der Master-Server für längere Zeit außer Betrieb ist, kann ein Replikationsserver zum Master-Server hochgestuft werden, damit Schreiboperationen für das Verzeichnis möglich sind.

## Policy Director-Überbrückungsfunktion für LDAP-Server

Policy Director stellt beim Start eine Verbindung zum LDAP-Master-Server her. Wenn der LDAP-Master-Server inaktiv ist, muss der Policy Director-Server in der Lage sein, eine Verbindung zu einem verfügbaren LDAP-Replikationsserver herzustellen, um Leseoperationen ausführen zu können.

Bei vielen Operationen, insbesondere Operationen regulärer Benutzer, handelt es sich um Leseoperationen. Hierzu gehören auch Operationen wie Benutzerauthentifizierung und -anmeldung an über eine Junction verbundenen Backend-Webservern. Nach der entsprechen-

den Konfiguration führt Policy Director eine Überbrückung zu einem Replikationsserver durch, wenn keine Verbindung zum Master-Server hergestellt werden kann.

Die Konfigurationsparameter für LDAP-Überbrückung finden Sie in der Zeilengruppe **[ldap]** der Konfigurationsdatei `ldap.conf`:

UNIX: `/opt/PolicyDirector/etc/ldap.conf`
Windows: `<Installationspfad>\etc\ldap.conf`

## Master-Serverkonfiguration

IBM SecureWay Directory (LDAP) unterstützt die Existenz eines einzelnen LDAP-Master-Servers für Lese-/Schreiboperationen. iPlanet Directory Server unterstützt mehrere LDAP-Server für Lese-/Schreiboperationen. Policy Director behandelt den iPlanet “Lieferantenserver” als Master-Server für Konfigurationszwecke.

Die aktiven Konfigurationszeilen in der Datei `ldap.conf` stellen die Parameter und Werte für diesen LDAP-Master-Server dar. Sie bestimmen diese Werte während der Policy Director-Konfiguration. Zum Beispiel:

```
[ldap]
enabled = yes
host = outback
port = 389
ssl-port = 636
max-search-size = 2048
```

| Parameter | Beschreibung |
|---|---|
| **enabled** | Policy Director verwendet eine LDAP-Benutzer-registrierungsdatenbank. Gültige Werte sind “yes” und “no”. |
| **host** | Der Netzname der Maschine, auf der sich der LDAP-Master-Server befindet. |
| **port** | Der TCP-Empfangs-Port des LDAP-Master-Servers. |
| **ssl-port** | Der SSL-Empfangs-Port des LDAP-Master-Servers. |

| Parameter | Beschreibung |
|---|---|
| **max-search-size** | Das Policy Director-Limit für eine LDAP-Client-Suche nach Datenbankeinträgen - z. B. eine Anforderung an die Management Console, Benutzer aus der LDAP-Datenbank aufzulisten. |

Wenn Sie eine Änderung an der LDAP-Datenbank vornehmen, z. B. ein neues Benutzerkonto über die Management Console hinzufügen, verwendet Policy Director immer den LDAP-Lese-/-Schreibserver (Master).

## Replikationsserverkonfiguration

IBM SecureWay Directory (LDAP) unterstützt die Existenz mindestens eines LDAP-Replikationsservers mit Lesezugriff. iPlanet Directory Server (LDAP) unterstützt die Existenz mindestens eines LDAP-Replikationsservers mit Lesezugriff, der als “Konsument” bezeichnet wird.

Sie müssen der Zeilengruppe **[ldap]** Zeilen hinzufügen, die alle Replikationsserver, die Policy Director zur Verfügung stehen, identifizieren. Verwenden Sie folgende Syntax für jeden Replikationsserver:

```
replica = <ldap-server>,<port>,<type>,<preference>
```

| Parameter | Beschreibung |
|---|---|
| **ldap-server** | Der Netzname des LDAP-Replikationsservers. |
| **port** | Der Empfangs-Port dieses Servers. Verwenden Sie normalerweise 389 oder 636. |
| **type** | Die Funktionalität des Replikationsservers - entweder “Lesen” oder “Lesen/Schreiben”. Verwenden Sie normalerweise “Lesen”. “Lesen/Schreiben” wird für einen Master-Server verwendet. |
| **preference** | Eine Zahl von 1 - 10. Der Server mit dem höchsten Prioritätswert wird für LDAP-Verbindungen ausgewählt. Siehe „Prioritätswerte für LDAP-Replikationsserver definieren” auf Seite 161. |

Beispiel:

```
replica = replica1.ldap.tivoli.com,389,readonly,5
replica = replica2.ldap.tivoli.com,389,readonly,5
```

Änderungen in der Datei `ldap.conf` werden erst wirksam, wenn Sie Policy Director erneut starten.

## Prioritätswerte für LDAP-Replikationsserver definieren

Jeder LDAP-Replikationsserver muss über einen Prioritätswert (1-10) verfügen, der seine Rangordnung festlegt bei der Auswahl als:

- Primärer Lesezugriffsserver oder
- Sicherungslesezugriffsserver für eine Überbrückung

Je höher die Zahl, desto höher die Priorität. Wenn der primäre Lesezugriffsserver ausfällt, wird der Server mit dem nächsthöheren Prioritätswert verwendet. Verfügen mehrere Server über denselben Prioritätswert, wird durch einen Lastausgleichsalgorithmus bestimmt, welcher ausgewählt wird.

Denken Sie daran, dass der LDAP-Master-Server als Server mit Lesezugriff und als Server mit Lese-/Schreibzugriff dienen kann. Für den Lesezugriff verfügt der Master-Server über die fest codierte Prioritätseinstellung 5. Dadurch können Sie für die Replikationsserver einen höheren oder niedrigeren Wert als für den Master angeben, um die erforderliche Leistung zu erzielen. Mit den entsprechenden Prioritätseinstellungen könnten Sie beispielsweise verhindern, dass der Master-Server tägliche Leseoperationen ausführt.

Sie können hierarchische Prioritätswerte definieren, um den Zugriff auf einen einzelnen LDAP-Server zu gestatten (mit Überbrückung zu den anderen Servern), oder Sie können gleiche Prioritäten für alle Server definieren, damit die Serverauswahl durch den Lastausgleich bestimmt wird.

Die folgende Tabelle illustriert einige mögliche Prioritätsszenarios. “M” bedeutet LDAP-Master-Server (Lesen, Lesen/Schreiben), und “R1, R2, R3” gibt die LDAP-Replikationsserver (Lesen) an.

| M | R1 | R2 | R3 | Überbrückungspriorität |
|---|---|---|---|---|
| **5** | **5** | **5** | **5** | Alle Server haben denselben Prioritätswert. Der Lastausgleich bestimmt, welcher Server für die jeweilige Zugriffsoperation ausgewählt wird. |
| **5** | **6** | **6** | **6** | Die drei Replikationsserver haben denselben Prioritätswert. Dieser Wert ist höher als der des Master-Servers. Der Lastausgleich bestimmt die Serverauswahl unter den drei Replikationsservern. Der Master-Server wird nur verwendet, wenn alle drei Replikationsserver nicht verfügbar sind. |
| **5** | **6** | **7** | **8** | Server 3 (mit dem höchsten Prioritätswert) wird zum primären Server. Wenn Server 3 ausfällt, wird Server 2 zum primären Server, weil dieser den nächsthöheren Prioritätswert hat. |

Die Prioritätswerte wirken sich nur auf den Lesezugriff für die LDAP-Datenbank aus. Policy Director verwendet immer den Master-Server (Lesen/Schreiben), wenn Sie eine Änderung in der LDAP-Datenbank vornehmen müssen.

Beachten Sie außerdem, dass einige Policy Director-Dämonen (z. B. der Management Server) die Prioritätseinstellungen in ihren Konfigurationsdateien überschreiben, um anzuzeigen, dass der Server für Lese-/Schreiboperationen bevorzugt wird. Der Grund hierfür ist, dass diese Dämonen in der Regel Aktualisierungsoperationen durchführen, die an den LDAP-Master-Server gehen sollten.

## Serversendeaufruf

Wenn ein LDAP-Server ausfällt, ruft Policy Director den Server ununterbrochen auf, um festzustellen, ob er wieder aktiv ist. Die Aufrufzeit beträgt 10 Sekunden.

# Policy Director-ACLs auf neue LDAP-Suffixe anwenden

**Anmerkung:** Die folgenden Informationen gelten sowohl für IBM SecureWay Directory Server als auch für iPlanet Directory Server.

Wenn ein LDAP-Administrator nach der Erstkonfiguration von Policy Director LDAP-Suffixe hinzufügt, muss der Administrator die entsprechenden Zugriffssteuerungslisten (Access Control Lists, ACLs) anwenden, damit Policy Director in der Lage ist, in diesen neuen Suffixen definierte Benutzer und Gruppen zu verwalten.

Verwenden Sie für IBM SecureWay Directory das Directory Management Tool zum Anwenden von ACLs. Verwenden Sie iPlanet Console 5.0 für Netscape LDAP-Server.

Verwenden Sie die entsprechende LDAP-Verwaltungsschnittstelle zum Anwenden der folgenden ACLs auf alle neuen Policy Director-Suffixe:

| LDAP-Gruppe | Zugriffssteuerung |
| --- | --- |
| **cn=SecurityGroup,secAuthority=Default** | |
| | ■ Uneingeschränkter Zugriff |
| **cn=ivacld-servers,cn=SecurityGroups,secAuthority=Default** | |
| | ■ Lesen<br>■ Suchen<br>■ Vergleichen |
| **cn=remote-acl-users,cn=SecurityGroups,secAuthority=Default** | |
| | ■ Lesen<br>■ Suchen<br>■ Vergleichen |

Diese Steuerangaben gelten, wenn der Administrator LDAP für die Policy Director-Benutzerregistrierungsdatenbank ausgewählt hat und ein neues LDAP-Suffix nach der Erstkonfiguration von Policy Director erstellt wurde. Es wird vorausgesetzt, dass Sie der Policy Director-Administrator sind und über Erfahrung mit Policy Director und LDAP verfügen. Außerdem wird vorausgesetzt, dass Sie als Administrator über die richtige Berechtigung zum Aktualisieren der LDAP-Verzeichnisinformationsbaumstruktur verfügen.

Wenn Policy Director konfiguriert wird, versucht es, auf jedes LDAP-Suffix, das zu diesem Zeitpunkt in dem LDAP-Server vorhanden ist, entsprechende ACLs anzuwenden. Mit Hilfe dieser Zugriffssteuerung kann Policy Director Benutzer- und Gruppeninformationen innerhalb dieser LDAP-Suffixe erstellen und verwalten.

Wird ein Suffix jedoch nach der Konfiguration von Policy Director erstellt und muss Policy Director später in der Lage sein, Benutzer- und Gruppeninformationen in diesem neuen Suffix zu erstellen und zu verwalten, müssen die entsprechenden Zugriffssteuerungen manuell angewendet werden. Ohne diese Zugriffssteuerungen hat Policy Director nicht die richtige LDAP-Berechtigung zum Erstellen und Verwalten von Benutzer- und Gruppeninformationen, die sich in diesem neuen Suffix befinden sollen.

Führen Sie je nach Art des LDAP-Servers (IBM SecureWay Directory Server oder iPlanet Directory Server) folgende Schritte aus, um die entsprechenden Zugriffssteuerungen auf das neu erstellte LDAP-Suffix anzuwenden.

Beachten Sie, dass bei den Prozeduren davon ausgegangen wird, dass das neu erstellte Suffix “**o=neworg,c=us**” heißt. Sie sollten diesen Wert in den folgenden Beschreibungen durch das tatsächlich neu erstellte Suffix ersetzen.

## Prozeduren für IBM SecureWay Directory Server

Die folgenden Schritte beschreiben, wie die entsprechenden Policy Director-Zugriffssteuerungen auf das neu erstellte Suffix für IBM SecureWay Directory Server angewendet werden.

1. Starten Sie das LDAP Directory Management Tool (DMT) mit einem der folgenden Befehle:

   Unter Windows: **Start -> Programme -> IBM SecureWay Directory -> Directory Management Tool**

   Unter UNIX:

   ```
   # /usr/bin/dmt
   ```

2. Möglicherweise wird folgende Warnung angezeigt:

   ```
   Warnung: Eintrag o=neworg,c=us enthält keine Daten.
   ```

   Entfernen Sie die Warnung. In Schritt 7 auf Seite 166 müssen Sie wissen, ob Sie diese Warnung gesehen haben.

3. Klicken Sie auf **Server hinzufügen** im linken Teilfenster. Das Fenster ’Server hinzufügen’ wird angezeigt.

4. Geben Sie die folgenden Werte in die folgenden Felder ein:

| Feld | Wert | Kommentar |
|---|---|---|
| Server-Name: | ldap://<Host-Name> | Zum Beispiel: ibm007.ibm.com |
| Port: | 389 | 389 ist der Standard-Port |
| Registrierter Benutzername: | cn=root | DN des LDAP-Administrators |
| Benutzerkennwort: | abc123 | Kennwort des LDAP-Administrators |

5. Klicken Sie auf **OK**. Die Seite des Directory Management Tools wird angezeigt.

6. Überprüfen Sie den Servernamen im oberen Teil des linken Fensters. Zum Beispiel: `ldap://ibm007.ibm.com:389`

7. Wählen Sie in der Baumstruktur auf der linken Seite **Verzeichnisstruktur > Baumstruktur anzeigen** aus.

   Möglicherweise wird folgende Warnung angezeigt:

   ```
   Warnung: Eintrag o=neworg,c=us enthält keine Daten.
   ```

8. Wenn Sie die folgende Nachricht nicht gesehen haben, fahren Sie mit Schritt 9 fort:

   ```
   Warnung: Eintrag o=neworg,c=us enthält keine Daten.
   ```

   Wenn Sie diese Nachricht gesehen haben, müssen Sie einen Eintrag für das Suffix erstellen. Auf das Suffix kann erst dann eine Zugriffssteuerung angewendet werden, wenn ein Eintrag vorhanden ist. Gehen Sie wie folgt vor, um einen Eintrag zu erstellen:

   a. Klicken Sie auf **Hinzufügen** im rechten Teilfenster. Das Dialogfenster zum Hinzufügen eines LDAP-Eintrags wird angezeigt.

   b. Geben Sie **Organisation** als Eintragsart an. Definieren Sie c=us als übergeordneten registrierten Namen. Geben Sie o=neworg als registrierten Eintragsnamen an. Klicken Sie auf **OK**. Die Eintragsseite für ’Organisation’ wird im Dialogfenster zum Hinzufügen eines LDAP-Eintrags angezeigt.

   c. Geben Sie den Organisationsnamen (neworg) im Abschnitt **Attribute** bei **`o:`** ein.

   d. Klicken Sie auf **Hinzufügen**. Die Seite ’Verzeichnisbaumstruktur anzeigen’ wird angezeigt.

9. Klicken Sie auf **Verzeichnisstruktur -> Baumstruktur aktualisieren** im linken Teilfenster.

10. Heben Sie das neu erstellte Suffix im Teilfenster ’Baumstruktur anzeigen’ auf der rechten Seite hervor.
11. Klicken Sie auf **ACL** im rechten Teilfenster. Die aktuellen Einstellungen der Zugriffssteuerungsliste (ACL) für das Suffix werden im Fenster ’LDAP-Zugriffssteuerungsliste bearbeiten’ angezeigt.
12. Geben Sie im Subjektbereich des Fensters ’LDAP-Zugriffssteuerungsliste bearbeiten’ folgenden registrierten Namen ein:

    ```
    cn=SecurityGroup,secAuthority=Default
    ```

    Wählen Sie die Gruppenart aus und klicken Sie auf **Hinzufügen**.
13. Wenn das Fenster angezeigt wird, wählen Sie folgendes aus:
    - Wählen Sie **Untergeordnete Einträge der Verzeichnisstruktur erben vom Eintrag** im Feld **DN-Eintrag** aus.
    - Wählen Sie im Feld **Berechtigungen** für **Untergeordneten Eintrag hinzufügen** und **Eintrag löschen Erteilen** aus.
    - Wählen Sie im Feld **Sicherheitsklasse** für jede Sicherheitsklasse (**Normal**, **Sensibel** und **Kritisch**) **Erteilen** für jede Berechtigung (**Lesen**, **Schreiben**, **Suchen** und **Vergleichen**) aus.

    Klicken Sie auf **OK**.
14. Heben Sie das neu erstellte Suffix im Teilfenster **Baumstruktur anzeigen** auf der rechten Seite hervor.
15. Klicken Sie auf **ACL** im rechten Teilfenster. Überprüfen Sie, ob die Gruppe **cn=SecurityGroup,secAuthority=Default** aufgeführt ist und die Einstellungen der Gruppe korrekt sind. Bei Gruppennamen muss die Groß-/Kleinschreibung nicht beachtet werden.

16. Geben Sie im Subjektbereich des Fensters 'LDAP-Zugriffssteuerungsliste bearbeiten' folgenden registrierten Namen ein:

    ```
    cn=ivacld-servers,cn=SecurityGroups,secAuthority=Default
    ```

    Wählen Sie die Gruppe **Typ** aus und klicken Sie auf **Hinzufügen**.

17. Wenn das Fenster angezeigt wird, wählen Sie folgendes aus:

    - Wählen Sie **Untergeordnete Einträge der Verzeichnisstruktur erben vom Eintrag** im Feld **DN-Eintrag** aus.
    - Wählen Sie im Feld **Berechtigungen** für **Untergeordneten Eintrag hinzufügen** und **Eintrag löschen Nicht spezifiziert** aus.
    - Wählen Sie im Feld **Sicherheitsklasse** für die Sicherheitsklasse **Normal Erteilen** für die Berechtigungen **Lesen**, **Suchen** und **Vergleichen** aus.
    - Wählen Sie im Feld **Sicherheitsklasse** für die Sicherheitsklasse **Normal Nicht spezifiziert** für die Berechtigung **Schreiben** aus.
    - Wählen Sie im Feld **Sicherheitsklasse** für die Sicherheitsklassen **Sensibel** und **Kritisch Nicht spezifiziert** für alle Berechtigungen aus.

    Klicken Sie auf **OK**.

18. Heben Sie das neu erstellte Suffix im Teilfenster **Baumstruktur anzeigen** auf der rechten Seite hervor. Klicken Sie auf **ACL** im rechten Teilfenster. Überprüfen Sie, ob die Gruppe **cn=ivacld-servers,cn=SecurityGroups,secAuthority=Default** aufgeführt ist und die Einstellungen der Gruppe korrekt sind. Bei Gruppennamen muss die Groß-/Kleinschreibung nicht beachtet werden.

19. Geben Sie im Subjektbereich des Fensters ’LDAP-Zugriffs-steuerungsliste bearbeiten’ folgenden registrierten Namen ein:

    ```
    cn=remote-acl-users,cn=SecurityGroups,secAuthority=Default
    ```

    Wählen Sie die Gruppe **Typ** aus und klicken Sie auf **Hinzufügen**.

20. Wenn das Fenster angezeigt wird, wählen Sie folgendes aus:

    - Wählen Sie **Untergeordnete Einträge der Verzeichnisstruktur erben vom Eintrag** im Feld **DN-Eintrag** aus.
    - Wählen Sie im Feld **Berechtigungen** für **Untergeordneten Eintrag hinzufügen** und **Eintrag löschen Nicht spezifiziert** aus.
    - Wählen Sie im Feld **Sicherheitsklasse** für die Sicherheitsklasse **Normal Erteilen** für die Berechtigungen **Lesen**, **Suchen** und **Vergleichen** aus.
    - Wählen Sie im Feld **Sicherheitsklasse** für die Sicherheitsklasse **Normal Nicht spezifiziert** für die Berechtigung **Schreiben** aus.
    - Wählen Sie im Feld **Sicherheitsklasse** für die Sicherheitsklassen **Sensibel** und **Kritisch Nicht spezifiziert** für alle Berechtigungen (**Lesen**, **Schreiben**, **Suchen** und **Vergleichen**) aus.

    Klicken Sie auf **OK**.

21. Klicken Sie auf **Beenden**, um das Directory Management Tool zu schließen.

## Prozeduren für iPlanet Directory Server

Diese Prozeduren beschreiben die Erstellung von ACLs für Suffixe mit Hilfe von iPlanet Console 5.0.

1. Starten Sie iPlanet Console 5.0 mit einem der folgenden Befehle:
   - Geben Sie auf UNIX-Systemen folgendes im Installationsverzeichnis von iPlanet Directory Server ein:

     ```
     # ./startconsole
     ```
   - Klicken Sie auf Windows-Systemen auf **Start -> Programme -> iPlanet Server-Produkte -> iPlanet Console 5.0**
2. Geben Sie die Benutzer-ID des LDAP-Administrators ein. Dies ist normalerweise **cn=Directory Manager**. Geben Sie das Kennwort und die Verwaltungs-URL ein. Klicken Sie auf **OK**.
3. Wählen Sie die Domäne aus, die Policy Director verwenden soll.
4. Erweitern Sie den Servernamen und **Servergruppe**.
5. Wählen Sie den Eintrag **Directory Server** aus. Konfigurationsdaten zum iPlanet Directory Server werden angezeigt.
6. Klicken Sie auf **Öffnen**. Es wird auf den iPlanet Directory Server zugegriffen.
7. Klicken Sie auf die Registerkarte **Directory**. Wird das neu erstellte Suffix im linken Teilfenster angezeigt, fahren Sie mit Schritt 8 auf Seite 171 fort.

   Wird das neu erstellte Suffix nicht im linken Teilfenster angezeigt, müssen Sie einen Eintrag für das neue Suffix erstellen, bevor Sie Zugriffssteuerungen auf das Suffix anwenden. Gehen Sie wie folgt vor, um den Eintrag zu erstellen:

a. Heben Sie den Namen des Servers am Anfang der Verzeichnisbaumstruktur hervor. Klicken Sie auf **Object** -> **New Root Object**. Ein Liste der Root-Suffixe wird angezeigt.

b. Wählen Sie **o=neworg,c=us** aus der Liste der Root-Suffixe aus. Das Auswahlfenster ’New Object’ wird angezeigt.

c. Blättern Sie im Auswahlfenster ’New Object’ vorwärts und wählen Sie **Organization** als neue Objekteintragsart aus.

d. Klicken Sie auf **OK**. Das Merkmaleditierfenster wird angezeigt.

e. Geben Sie **neworg** in das Feld ’Organization’ ein und klicken Sie auf **OK**.

**Anmerkung:** In diesen Anweisungen wird ein Beispielsuffix verwendet. Wenn Sie ein Suffix erstellen, müssen Sie die tatsächliche Eintragsart und den tatsächlichen Namen angeben.

f. Klicken Sie auf **View** -> **Refresh**. Der neue Suffixeintrag wird im linken Teilfenster angezeigt.

8. Heben Sie den Eintrag **neworg** im linken Teilfenster hervor. Klicken Sie auf **Object -> Set Access Permissions**. Das Fenster ’Manage Access Control’ für o=neworg,c=us wird angezeigt.
9. Klicken Sie auf **New**, um das Fenster ’Edit ACI for o=neworg, c=us’ anzuzeigen.
10. Geben Sie `SECURITY GROUP - ALLOW ALL` als ACI-Namen an.
11. Heben Sie den Namen ’All Users’ hervor und klicken Sie auf **Remove**.
12. Klicken Sie auf **Edit Manually**. Das Fenster ’Edit ACI for o=neworg,c=us’ wird angezeigt.

13. Ersetzen Sie den Standard-ACI-Text durch den folgenden:

```
(target="ldap:///o=neworg,c=us")(targetattr="*")
(version 3.0; acl "SECURITY GROUP - ALLOW ALL";
allow (all)
groupdn = "ldap:///cn=SecurityGroup,secAuthority=Default";)
```

    Klicken Sie auf **Check Syntax**, um sicherzustellen, dass Sie den Text korrekt eingegeben haben. Korrigieren Sie alle Fehler, bis die Syntaxanalyse fehlerfrei ist.

14. Klicken Sie auf **OK**. Das Fenster 'Manage Access Control' für o=neworg,c=us wird angezeigt.
15. Klicken Sie auf **Neu**. Geben Sie folgenden ACI-Namen an:

```
PD Servers GROUP - ALLOW READ
```

16. Heben Sie den Namen 'All Users' hervor und klicken Sie auf **Remove**.
17. Klicken Sie auf **Edit Manually**. Das Fenster 'Edit ACI for o=neworg,c=us' wird angezeigt.
18. Ersetzen Sie den Standard-ACI-Text durch den folgenden:

```
(target="ldap:///o=neworg,c=us")(targetattr="*")
(version 3.0; acl "SECURITY GROUP - ALLOW READ";
allow(read, search, compare)
groupdn = "ldap:///cn=ivacld-servers,
cn=SecurityGroups,secAuthority=Default";)
```

    Klicken Sie auf **Check Syntax**, um sicherzustellen, dass Sie den Text korrekt eingegeben haben. Korrigieren Sie alle Fehler, bis die Syntaxanalyse fehlerfrei ist.

19. Klicken Sie auf **OK**. Das Fenster 'Manage Access Control' für o=neworg,c=us wird angezeigt.
20. Klicken Sie auf **Neu**. Geben Sie den ACI-Namen `PD Remote ACL Users GROUP -ALLOW READ` an.
21. Heben Sie den Namen 'All Users' hervor und klicken Sie auf **Remove**.
22. Klicken Sie auf **Edit Manually**. Das Fenster 'Edit ACI for o=neworg,c=us' wird angezeigt.

23. Ersetzen Sie den Standard-ACI-Text durch den folgenden:

```
(target="ldap:///o=neworg,c=us")(targetattr="*")
(version 3.0; acl "SECURITY GROUP - ALLOW READ";
allow (read, search, compare)
groupdn = "ldap:///cn=remote-acl-users,
cn=SecurityGroups,secAuthority=Default";)
```

    Klicken Sie auf **Check Syntax**, um sicherzustellen, dass Sie den Text korrekt eingegeben haben. Korrigieren Sie alle Fehler, bis die Syntaxanalyse fehlerfrei ist.

24. Klicken Sie auf **OK**. Das Fenster ’Manage Access Control’ für o=neworg,c=us wird angezeigt.

25. Klicken Sie auf **Neu**. Geben Sie den ACI-Namen `PD Deny-Others1` an.

26. Heben Sie den Namen ’All Users’ hervor und klicken Sie auf **Remove**.

27. Klicken Sie auf **Edit Manually**. Das Fenster ’Edit ACI for o=neworg,c=us’ wird angezeigt.

28. Ersetzen Sie den Standard-ACI-Text durch den folgenden:

```
(targetfilter="(|(objectclass=secUser)
(objectclass=secGroup))")
(version 3.0; acl "PD Deny-Others"; deny(all)
groupdn != "ldap:///cn=SecurityGroup,secAuthority=Default ||
ldap:///cn=remote-acl-users,
cn=SecurityGroups,secAuthority=Default ||
ldap:///cn=ivacld-servers,
cn=SecurityGroups,secAuthority=Default";)
```

    Klicken Sie auf **Check Syntax**, um sicherzustellen, dass Sie den Text korrekt eingegeben haben. Korrigieren Sie alle Fehler, bis die Syntaxanalyse fehlerfrei ist.

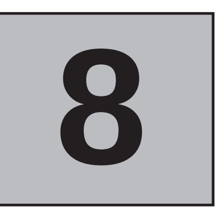
29. Klicken Sie auf **OK**. Das Fenster ’Manage Access Control’ für o=neworg,c=us wird angezeigt.

30. Klicken Sie auf **Neu**. Geben Sie den ACI-Namen `PD Deny-Others2` an.

31. Heben Sie den Namen ’All Users’ hervor und klicken Sie auf **Remove**.
32. Klicken Sie auf **Edit Manually**. Das Fenster ’Edit ACI for o=neworg,c=us’ wird angezeigt.
33. Ersetzen Sie den Standard-ACI-Text durch den folgenden:

    ```
    (targetfilter="(|(objectclass=secPolicyData)
    (objectclass=secPolicy))")
    (version 3.0; acl "PD Deny-Others"; deny(all)
    groupdn != "ldap:///cn=SecurityGroup,secAuthority=Default ||
    ldap:///cn=remote-acl-users,
    cn=SecurityGroups,secAuthority=Default ||
    ldap:///cn=ivacld-servers,
    cn=SecurityGroups,secAuthority=Default";)
    ```

    Klicken Sie auf **Check Syntax**, um sicherzustellen, dass Sie den Text korrekt eingegeben haben. Korrigieren Sie alle Fehler, bis die Syntaxanalyse fehlerfrei ist.
34. Klicken Sie auf **OK**. Das Fenster ’Manage Access Control’ für o=neworg,c=us wird angezeigt.
35. Klicken Sie auf **OK**, um das Fenster ’Manage Access Control’ für o=neworg,c=us zu schließen.
36. Klicken Sie auf **Console -> Exit**, um die Konsole zu verlassen.



# Serveraktivität protokollieren und prüfen



Policy Director stellt eine Reihe von Protokoll- und Prüffunktionen zur Verfügung. Protokolldateien können alle Fehlernachrichten und Warnungen, die Policy Director-Server generieren, erfassen. Prüfprotokolldateien können Berechtigung, Authentifizierung, Verwaltung und auf den Policy Director-Servern auftretende HTTP-Ereignisse erfassen.

Stichwortindex:



## Einführung in Protokollieren und Prüfen

Der Inhalt der Protokoll- und Prüfprotokolldateien kann eine nützliche Informationsquelle für die Überwachung und Fehlerbehebung der Aktivität von Policy Director-Servern darstellen.

## Protokolldateien

In den Protokolldateien speichern Policy Director-Server Warnungen und Fehlernachrichten. Alle Protokolldateien haben ein ASCII-Format.

Policy Director stellt folgende Protokolldateien zur Verfügung:

1. Policy Director-Serverprotokolldateien

   Siehe „Policy Director-Serverprotokolldateien" auf Seite 177.

2. Servicenachrichten

   Siehe „Servicenachrichten" auf Seite 178.

## Prüfprotokolldateien

In den Prüfprotokolldateien speichern die Policy Director-Server Sätze der Serveraktivität. Die Ausgabe eines bestimmten Serverereignisses wird als Satz bezeichnet. Ein Prüfprotokoll ist eine Sammlung mehrerer Sätze, die die Serveraktivität dokumentieren. Alle Policy Director-Prüfprotokolldateien haben ein ASCII-Format.

Policy Director-Prüfprotokolldateien zeichnen Ereignisse für folgende Server auf:

- Management Server (**pdmgrd**)
- Authorization Server (**pdacld**)
- WebSEAL (**websealdd**)

Siehe „Policy Director-Prüfprotokolldateien" auf Seite 180.

Siehe „Prüfprotokolldateiformat" auf Seite 184.

Siehe „Inhalt der Prüfprotokolldatei" auf Seite 186.

## Dokumentationskonvention: <Installationspfad>

Die in diesem Kapitel verwendete Variable **<Installationspfad>** wird, gemäß der Betriebssystemplattform, wie folgt interpretiert:

UNIX: `/opt/PolicyDirector/`
Windows: `\Program Files\Tivoli\Policy Director`

Dieser Pfadname ist in UNIX fest und kann nicht geändert werden.

Unter Windows können Sie den **<Installationspfad>** während der Installation der Policy Director-Software definieren.

# Policy Director-Serverprotokolldateien

Jeder Policy Director-Server generiert Warnungen und Fehlernachrichten dynamisch. Diese Nachrichten werden an Standardfehler übertragen und dann an spezifische Protokolldateien umgeleitet.

| Server | Protokolldateiposition |
|---|---|
| Management Server (pdmgrd) | (Parameter in Konfigurationsdatei `ivmgrd.conf`.)<br>UNIX:<br>log-file=/var/PolicyDirector/log/pdmgrd.log<br>Windows:<br>log-file=<*Installationspfad*>\log\pdmgrd.log |
| Authorization Server (pdacld) | (Parameter in Konfigurationsdatei `ivacld.conf`.)<br>UNIX:<br>log-file=/var/PolicyDirector/log/pdacld.log<br>Windows:<br>log-file=<*Installationspfad*>\log\pdacld.log |
| WebSEAL (webseald) | (Parameter in Konfigurationsdatei `webseald.conf`.)<br>UNIX:<br>log-file=/var/PolicyDirector/log/webseald.log<br>Windows:<br>log-file=<*Installationspfad*>\log\webseald.log |

## Policy Director-Serverprotokolldateien aktivieren und inaktivieren

Das Protokollieren ist aktiviert, wenn in der Konfigurationsdatei für den betreffenden Server eine Protokolldatei definiert ist.

## Beispiel: ivmgrd.log

```
2001-08-18-20:03:26.231+00:00I----- 0x1354A0A0 pdmgrd NOTICE ivc
general ivmgrd.
cpp 720 0x00000001
Datenbank öffnen
2001-08-18-20:03:26.232+00:00I----- 0x1354A0A0 pdmgrd NOTICE ivc
general ivmgrd.
cpp 727 0x00000001
Datenbank wird erstellt
2001-08-18-20:03:26.312+00:00I----- 0x1354A0A0 pdmgrd NOTICE ivc
general ivmgrd.
cpp 749 0x00000001
Client-Benachrichtigungsfunktion initialisieren
2001-08-18-20:03:26.315+00:00I----- 0x1354A0A0 pdmgrd NOTICE ivc
general ivmgrd.
cpp 760 0x00000001
Lokalen Objekt-Cache initialisieren
2001-08-18-20:03:26.728+00:00I----- 0x1354A0A0 pdmgrd NOTICE ivc
general ivmgrd.
cpp 825 0x00000001
Berechtigungsmanager initialisieren
2001-08-18-20:03:29.278+00:00I----- 0x1354A0A0 pdmgrd NOTICE ivc
general ivmgrd.
cpp 833 0x00000001
Client-Berechtigung initialisieren
2001-08-18-20:03:31.341+00:00I----- 0x1354A0A0 pdmgrd NOTICE ivc
general ivmgrd.
cpp 863 0x00000001
Server-Manager initialisieren
2001-08-18-20:03:31.345+00:00I----- 0x1354A0A0 pdmgrd NOTICE ivc
general ivmgrd.
cpp 872 0x00000001
Befehlssteuerroutine initialisieren
cpp 937 0x000000012.799+00:00I----- 0x1354A0A0 pdmgrd NOTICE ivc
general ivmgrd.
Server bereit
pp 528 0x0000001335.377+00:00I----- 0x10652105 pdmgrd NOTICE bas
mts mtsserver.c
Der Server ist an Port 7135 empfangsbereit.
```

## Servicenachrichten

Servicenachrichten werden durch die `Routing`-Datei gesteuert:

UNIX: `/opt/PolicyDirector/etc/routing`
Windows: `<`*`Installationspfad`*`>\etc\routing`

Einträge in dieser Konfigurationsdatei legen die Art der Informationen, die protokolliert werden, fest. Die `Routing`-Datei enthält folgende Standardeinträge:

**UNIX:**

```
FATAL:STDOUT:-;FILE:/var/PolicyDirector/log/fatal.log
ERROR:STDOUT:-;FILE:/var/PolicyDirector/log/error.log
WARNING:STDOUT:-;FILE:/var/PolicyDirector/log/warning.log
NOTICE:FILE.10.100:/var/PolicyDirector/log/notice.log
```

**Windows:**

```
FATAL:STDERR:-;FILE:%PDDIR%/log/fatal.log
ERROR:STDERR:-;FILE:%PDDIR%/log/error.log
WARNING:STDERR:-;FILE:%PDDIR%/log/warning.log
NOTICE:FILE.10.100:%PDDIR%/log/notice.log
```

## Nachrichten an Standardausgabe übertragen

Warnungen und Fehlernachrichten (einschließlich NOTICE-Nachrichten) werden normalerweise an die entsprechenden Protokolldateien umgeleitet.

Sollen diese Nachrichten an die Standardausgabe (Terminal) übertragen werden, verwenden Sie den Befehl **-foreground** beim Starten eines Servers. Hierdurch wird der Server im Vordergrund ausgeführt (das heißt, der Server dämonisiert sich nicht selbst), und Warnungen und Fehlernachrichten werden an die Standardausgabe gesendet.

Soll der Management Server z. B. im Debug-Modus gestartet werden, geben Sie folgenden Befehl ein:

```
# /opt/PolicyDirector/bin/pdmgrd -foreground
```

Sie können die Serverausgabe auch mit dem UNIX-Befehl **tee** in einer einzelnen Datei erfassen.

Das folgende Beispiel zeigt, wie der Management Server in diesem Modus gestartet wird:

```
# pdmgrd -foreground 2>&1 | tee /tmp/ivmgrd.log
```

### Hinweise zum Debug-Modus

1. Wenn Sie die Erfassung der Informationen zur Serveraktivität abgeschlossen haben, müssen Sie darauf achten, dass die normale Bedingung der Routing-Datei wiederhergestellt wird. Entfernen Sie den NOTICE-Eintrag. NOTICE generiert sehr viele Informationen, die sich schnell ansammeln.
2. Mit der Tastenkombination **Strg + c** können Sie einen Serverprozess, der im Debug-Modus gestartet wurde, unterbrechen. Der Serverprozess wird korrekt abgeschlossen und beendet.

## Policy Director-Prüfprotokolldateien

Die Prüfung ist definiert als das Erfassen von Daten zu Systemaktivitäten, die die sichere Verarbeitung des Policy Director-Berechtigungsprozesses beeinflussen. Jeder Policy Director-Server kann Prüfereignisse erfassen, sobald eine sicherheitsbezogene, prüfbare Aktivität auftritt.

Prüfereignisse werden als Prüfsätze gesichert, die die spezifische Aktivität dieses Server dokumentieren. Jede geprüfte Aktivität wird als **Prüfereignis** bezeichnet. Eine Sammlung von Prüfereignissätzen, die in einer Datei gespeichert werden, wird als **Prüfprotokoll** bezeichnet.

Jeder Policy Director-Server verwaltet seine eigene Prüfprotokolldatei. Der Policy Director-Server enthält:

- Management Server (**pdmgrd**)
- Authorization Server (**pdacld**)
- WebSEAL (**webseald**)
- Benutzererstellte Anwendungen unter Verwendung von Authorization ADK (Siehe Handbuch *Tivoli SecureWay Policy Director Authorization ADK Developer Reference*)

Die Parameter für die Konfiguration der Policy Director-Serverprüfprotokolldateien befinden sich in der Zeilengruppe **[aznapi-configuration]** in jeder der Dateien `<Servername>.conf`.

| Server | Servername | Konfigurationsdatei |
|---|---|---|
| Management Server | **pdmgrd** | ivmgrd.conf |
| Authorization Server | **pdacld** | ivacld.conf |
| WebSEAL | **webseald** | webseald.conf |

## Prüfung aktivieren und inaktivieren

Die Prüfprotokollaufzeichnung wird auf Serverbasis durch Definieren des Werts **logaudit** in der Zeilengruppe **[aznapi-configuration]** der Konfigurationsdatei für den spezifischen Server aktiviert.

Die Prüfung ist standardmäßig inaktiviert:

```
[aznapi-configuration]
logaudit = no
```

Der Wert “yes” aktiviert die Prüfung für diesen Server. Zum Beispiel:

```
[aznapi-configuration]
logaudit = yes
```

## Protokolldateiposition angeben

Die Prüfprotokolldatei für jeden Server hat standardmäßig den Namen `audit.log` und befindet sich im Protokollverzeichnis des betreffenden Servers.Der Parameter **auditlog** in der Konfigurationsdatei der einzelnen Server gibt die Position der Prüfprotokolldatei an:

| Server | Protokolldateiposition |
|---|---|
| Management Server (**pdmgrd**) | UNIX: `auditlog=/var/PolicyDirector/audit/pdmgrd.log`<br>Windows: `auditlog=C:\pd\audit\pdmgrd.log` |
| Authorization Server (**pdacld**) | UNIX: `auditlog=/var/PolicyDirector/audit/pdacld.log`<br>Windows: `auditlog=C:\pd\audit\pdacld.log` |

## Überlaufschwellenwerte für Prüfprotokolldateien angeben

Der Parameter **logsize** gibt die maximale Größe an, bis zu der Prüfprotokolldateien anwachsen können. Er hat folgenden Standardwert (in Bytes):

```
[aznapi-configuration]
logsize = 2000000
```

Wenn eine Prüfprotokolldatei den angegebenen Wert erreicht — dieser wird als Überlaufschwellenwert bezeichnet — wird die vorhandene Datei unter demselben Namen, dem ein aktuelles Datum und eine Zeitmarke angefügt wird, gesichert. Dann wird eine neue Prüfprotokolldatei gestartet.

Die verschiedenen möglichen Werte für **logsize** werden wie folgt interpretiert:

- Wenn der Wert für **logsize** kleiner als Null ist (< 0), wird eine neue Prüfprotokolldatei bei jedem Aufruf des Prüfungsprozesses und alle 24 Stunden von diesem Exemplar erstellt.
- Wenn der Wert für **logsize** gleich Null ist (= 0), gibt es keinen Überlaufschwellenwert, und die Größe der Prüfprotokolldatei ist unbegrenzt. Wenn eine Prüfprotokolldatei bereits vorhanden ist, werden ihr neue Daten hinzugefügt.
- Wenn der Wert für **logsize** größer als Null ist (> 0), erfolgt ein Überlauf, wenn eine Prüfprotokolldatei den konfigurierten Schwellenwert erreicht. Wenn eine Prüfprotokolldatei beim Systemstart bereits vorhanden ist, werden ihr neue Daten hinzugefügt.

## Häufigkeit für das zwangsweise Schreiben in Prüfprotokolldateipuffer angeben

Prüfprotokolldateien werden in gepufferte Datenströme geschrieben. Wenn Sie die Prüfprotokolldateien in Echtzeit überwachen, können Sie die Häufigkeit, mit der der Server ein zwangsweises Schreiben in die Prüfprotokolldateipuffer erzwingt, ändern.

Standardmäßig erfolgt ein zwangsweises Schreiben der Prüfprotokolldateien alle 20 Sekunden:

```
[aznapi-configuration]
logflush = 20
```

Wenn Sie einen negativen Wert angeben, wird ein zwangsweises Schreiben nach dem Schreiben jedes Satzes erzwungen.

## Prüfereignisse angeben

Prüfereignisse werden nach der Serverfunktionalität, die sie generiert, kategorisiert. Einige Funktionen sind in allen Policy Director-Servern gleich, andere sind serverspezifisch. Jede Art der Serverfunktionalität ist einem Prüfbefehl zugeordnet:

| Prüfbefehl | Serverfunktionalität |
|---|---|
| **authn** | Authentifizierungsprüfung der Berechtigungs-anforderung |
| **azn** | Berechtigungsereignisprüfung |
| **mgmt** | Verwaltungsbefehlsprüfung |
| **http** | Webseal-HTTP-Anforderungsprüfung |

Sie können jeden Policy Director-Server so konfigurieren, dass er Prüfereignisse selektiv auf Kategoriebasis erfasst. Bei der folgenden Konfiguration werden beispielsweise nur Authentifizierungsereignisse erfasst, und die Erfassung aller anderen Ereignisse wird inaktiviert, einschließlich des Überschreibens jeder Berechtigungsprüfung, die in POP-Einstellungen aktiviert ist.

```
[aznapi-configuration]
auditcfg = authn
```

Die folgenden Einstellungen aktivieren WebSEAL-HTTP-Anforderungs- und Berechtigungsprüfung, inaktivieren jedoch alle anderen Prüfkategorien für den WebSEAL-Server:

```
[aznapi-configuration]
auditcfg = http
auditcfg = authn
```

Wenn die Prüfung für einen Prozess ohne konfigurierte Prüfbefehle aktiviert ist, werden standardmäßig alle prüfbaren Ereignisse erfasst.

Die folgende Tabelle zeigt die Prüfereignisse (gekennzeichnet durch den Prüfbefehl), die für jeden spezifischen Policy Director-Server erfasst werden können:

| Prüfbefehl | webseald | pdmgrd | pdacld | authadk |
|---|---|---|---|---|
| **authn** | **X** | X | **X** | **X** |
| **azn** | **X** | X | **X** | **X** |
| **mgmt** | | **X** | | |
| **http** | **X** | | | |

## Prüfprotokolldateiformat

Prüfereignisse werden im Prüfprotokoll in einem Standardformat mit Hilfe von Befehlen im XML-Stil erfasst. Auch wenn XML nur ein Zwischenschritt bei der Ausgabe einer Präsentationssicht der Daten ist, hat die XML-Datei ein ASCII-Format und kann direkt gelesen oder zur weiteren Analyse an andere externe Syntaxanalysekomponenten übermittelt werden.

Ein vollständiges Prüfprotokoll stellt kein einzelnes XML-Dokument dar. Jedes Prüfereignis in der Datei wird als isolierter XML-Datenblock geschrieben. Jeder Datenblock entspricht den Regeln der XML-Standardsyntax.

Als Prüfadministrator wird von Ihnen erwartet, dass Sie Ereignisse nach Ihren eigenen Kriterien auswählen und extrahieren. Hierzu kann auch das erneute Formatieren jedes Ereignisses gehören, wobei eine entsprechende DTD (Document Type Definition, Dokumentartdefinition) oder ein entsprechendes Schema für das von Ihnen verwendete Analyse-Tool angewendet wird. DTD ist ein Zwischenformat, das eine Beschreibung der Daten, die erfasst werden können, zur Verfügung stellt.

Der folgende Abschnitt zeigt einen DTD-Vorschlag.

```
<!--audit_event.dtd -->
<!ELEMENT event (date, outcome, originator, accessor, target, data*)>
<!ATTLIST event
          rev CDATA "1.1"
          link CDATA #IMPLIED >
<!ELEMENT date (#PCDATA)>
<!ELEMENT outcome (#PCDATA)>
<!ATTLIST outcome
          status CDATA #IMPLIED>
```

```
<!ELEMENT originator (component, event, location)>
<!ATTLIST originator
          blade CDATA #REQUIRED>
<!ELEMENT component rev CDATA "1.0">
<!ELEMENT action (#PCDATA)>
<!ELEMENT location (#PCDATA)>
<!ELEMENT accessor (principal*)>
<!ATTLIST accessor
          name CDATA #REQUIRED>
<!ELEMENT principal (#PCDATA)>
<!ATTLIST principal
          auth CDATA #REQUIRED>
<!ELEMENT target (object, process?, azn?)>
<!ATTLIST target
          resource CDATA #REQUIRED>
<!ELEMENT object (#PCDATA)>
<!ELEMENT process (pid, rid, eid, uid, gid)>
<!ATTLIST process
          architecture (unix | nt) 'unix'>
<!ELEMENT pid #PCDATA>
<!ELEMENT rid #PCDATA>
<!ELEMENT eid #PCDATA>
<!ELEMENT uid #PCDATA>
<!ELEMENT gid #PCDATA>
<!ELEMENT azn (perm, result, qualifier)>
<!ELEMENT perm #PCDATA>
<!ELEMENT result #PCDATA>
<!ELEMENT qualifier #PCDATA>
<!ELEMENT data #PCDATA>
<!ATTLIST data
          tag CDATA #REQUIRED>
```

Da bei der Policy Director-Prüfung ein Standardsatzformat verwendet wird, sind nicht alle Felder für jedes aufgezeichnete Ereignis relevant. Im allgemeinen erfasst jedes Ereignis das Ergebnis einer Aktion, die ein Principal für ein Zielobjekt ausführt.

Informationen zu der Aktion, die Berechtigung des Principals, das Zielobjekt und das Ergebnis werden in einem Header mit allgemeinem Format des Prüfsatzes erfasst. Felder, die für ein bestimmtes Ereignis nicht relevant sind, können einen Standardwert enthalten. Zusätzliche ereignisspezifische Informationen können auch in einem Datenbereich mit freiem Format am Ende des Satzes aufgezeichnet werden.

Für die Entschlüsselung der Bedeutung bestimmter Datenwerte in den Sätzen sind unter Umständen gute Kenntnisse über den Policy Director-Code und die Policy Director-Architektur erforderlich.

### Statusattribut des Felds Outcome

Das Feld **outcome** enthält immer einen Policy Director-**Status**code und einen Ergebniswert. Gültige Ergebniswerte sind:

```
0 = SUCCESS
1 = FAILURE
2 = PENDING
3 = UNKNOWN
```

Sie können mit dem Befehl **pdadmin errtext** eine Interpretation für den Policy Director-Statuscode (412668954 im folgenden Beispiel) zur Verfügung stellen.

```
<outcome status="412668954">1</outcome>
```

### Ressourcenattribut des Felds Target

Das **Ressourcen**attribut des Felds **target** stellt eine grobe Kategorisierung des Zielobjekts dar:

```
0 = AUTHORISATION
1 = PROCESS
2 = TCB
3 = CREDENTIAL
5 = GENERAL
```

## Inhalt der Prüfprotokolldatei

### Berechtigungsprüfsätze

Berechtigungserteilung ist die Hauptfunktion der Policy Director-Server. Berechtigungsprüfsätze können erfasst werden, wenn einem Zielobjekt in der Policy Director-Berechtigungs-Policy-Datenbank (geschützter Objektbereich) eine POP-Policy zugeordnet ist, die Prüffunktionen aktiviert.

Siehe „Policies für geschützte Objekte verwenden” auf Seite 105.

Sie können die Prüfung für einen bestimmten Server konfigurieren, indem Sie “azn” der Prüfkonfigurationsliste in der Zeilengruppe **[aznapi-configuration]** der Serverkonfigurationsdatei hinzufügen:

```
[aznapi-configuration]
auditcfg = azn
```

Das folgende Beispiel zeigt einen Prüfsatz für das folgende Ereignis:

```
pdadmin> pop modify pop1 set audit-level all
```


```
<event rev="1.1">
<date>2001-08-05-16:25:08.341+00:00I-----</date>
<outcome status="0">0</outcome>
<originator blade="pdmgrd"><component rev="1.1">mgmt</component>
<action>13702</action>
<location>phaedrus</location>
</originator>
<accessor name="">
<principal auth="IV_LDAP_V3.0">sec_master</principal>
</accessor>
<target resource="5"><object></object></target>
<data>
"13702"
"pop1"
"pop1"
"false"
"15"
"0"
""
"0"
"0"
"0"
"127"
"1"
"0"
"0"
"0"
</data>
</event>
```


## Authentifizierungsprüfsätze

Die Authentifizierung eines Principals erfolgt außerhalb von Policy Director während der Berechtigungsanforderung. Policy Director kann Prüfsätze erfassen, in denen der Erfolg oder Misserfolg dieser Authentifizierungsversuche aufgezeichnet wird.

Sie können die Prüfung von Authentifizierungsversuchen konfigurieren, indem Sie “authn” der Prüfkonfigurationsliste in der Zeilengruppe **[aznapi-configuration]** der Serverkonfigurationsdatei hinzufügen:

```
[aznapi-configuration]
auditcfg = authn
```

Das folgende Beispiel zeigt ein Authentifizierungsereignis, das von WebSEAL aus für einen nicht authentifizierten Benutzer protokolliert wurde.

```
<event rev="1.1">
<date>2001-08-05-23:04:26.630+00:00I-----</date>
<outcome status="0">0</outcome>
<originator blade="webseald"><component>authn</component>
<event rev="1">0</event>
<location>location not specified</location>
</originator>
<accessor name="unknown">
<principal auth="invalid"></principal>
</accessor>
<target resource="5"><object></object></target>
<data>
</data>
</event>
```

## WebSEAL-Prüfsätze

Die Webserveraktivität kann wahlweise in der Prüfprotokolldatei zusätzlich zu den oder anstelle der HHTP-Standarddateien im allgemeinen Protokollformat, die im *Tivoli SecureWay Policy Director WebSEAL Administratorhandbuch* beschrieben werden, aufgezeichnet werden.

Sie können die Prüfung der WebSEAL-Aktivität konfigurieren, indem Sie “http” der Prüfkonfigurationsliste in der Zeilengruppe **[aznapi-configuration]** der Konfigurationsdatei des WebSEAL-Servers (`webseald.conf`) hinzufügen:

```
[aznapi-configuration]
auditcfg = http
```

Das folgende Beispiel zeigt einen HTTP-Zugriffsprüfsatz:

```
<event rev="1.1">
<date>2001-08-05-23:04:26.931+00:00I-----</date>
<outcome status="412668954">1</outcome>
<originator blade="webseald"><component>http</component>
<event rev="1">2</event>
<location>146.84.251.70</location>
</originator>
<accessor name="user not specified">
```

```
<principal auth="IV_DCE_V3.0">cell_admin</principal>
</accessor>
<target resource="5"><object>/pics/pd30.gif</object></target>
<data>
</data>
</event>
```

## Verwaltungsprüfsätze

Zu den Zuständigkeiten des Management Servers gehört die Verwaltung der Hauptberechtigungs-Policy-Datenbank. Diese Datenbank enthält die Beschreibung des geschützten Objektbereichs für die gesicherte Domäne, ACL- und POP-Policies sowie die Angabe, wo ACLs und POPs Objekten zugeordnet sind.

Sie können die Prüfung der Management Server-Aktivität konfigurieren, indem Sie "mgmt" der Prüfkonfigurationsliste in der Zeilengruppe **[aznapi-configuration]** der Konfigurationsdatei des Management Servers (`ivmgrd.conf`) hinzufügen:

```
[aznapi-configuration]
auditcfg = mgmt
```

Das folgende Beispiel zeigt einen Ereignissatz des folgenden Befehls **pdadmin**:

```
pdadmin> pop modify pop1 set audit-level all
<event rev="1.1">
<date>2001-08-05-23:01:37.078+00:00I-----</date>
<outcome status="0">0</outcome>
<originator blade="ivmgrd"><component>mgmt</component>
<event rev="1">3702</event>
<location>location not specified</location>
</originator>
<accessor name="user not specified">
<principal auth="IV_DCE_V3.0">cell_admin</principal>
</accessor>
<target resource="5"><object></object></target>
<data>
"2019"
"1002"
"pop1"
"0"
""
</data>
</event>
```

## Ereignisfeld-ID-Codes für Verwaltungsbefehle

Die Prüfsätze für Verwaltungsbefehle enthalten einen Ereignis-ID-Code, der einen der Policy Director-Verwaltungsbefehle (**pdadmin**) angibt. Befehlsargumente werden im Abschnitt **data** des Ereignissatzes in ihrem internen Format aufgelistet.

Beachten Sie, dass Befehle, die keine effektive Änderung des Datenbankstatus bewirken (z. B. **list** und **show**), nie erfasst werden.

| **ACL-Verwaltungsbefehle** | |
|---|---|
| ACL_LIST | 13000 |
| ACL_GET | 13001 |
| ACL_SET | 13002 |
| ACL_DELETE | 13003 |
| ACL_FIND | 13005 |
| ACTION_LIST | 13006 |
| ACTION_SET | 13007 |
| ACTION_DELETE | 13008 |
| ACTION_GROUPLIST | 13009 |
| ACTION_GROUPCREATE | 13010 |
| ACTION_GROUPDELETE | 13011 |
| ACTION_LISTGROUP | 13012 |
| ACTION_CREATEGROUP | 13013 |
| ACTION_DELETEGROUP | 13014 |
| **Objektverwaltungsbefehle** | |
| OBJSPC_CREATE | 13103 |
| OBJSPC_DELETE | 13104 |
| OBJSPC_LIST | 13105 |
| OBJ_CREATE | 13106 |
| OBJ_DELETE | 13107 |
| OBJ_MOD_SET_NAME | 13110 |
| OBJ_MOD_SET_DESC | 13111 |
| OBJ_MOD_SET_TYPE | 13112 |
| OBJ_MOD_SET_ISLF | 13113 |

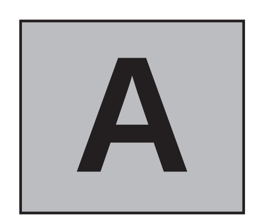
| | |
|---|---|
| OBJ_MOD_SET_ISPOL | 13114 |
| OBJ_MOD_SET_ATTR | 13115 |
| OBJ_MOD_DEL_ATTR | 13116 |
| OBJ_MOD_DEL_ATTRVAL | 13117 |
| OBJ_SHOW_ATTR | 13118 |
| OBJ_LIST_ATTR | 13119 |
| ACL_ATTACH | 13120 |
| ACL_DETACH | 13121 |
| ACL_MOD_SET_ATTR | 13123 |
| ACL_MOD_DEL_ATTR | 13124 |
| ACL_MOD_DEL_ATTRVAL | 13125 |
| ACL_SHOW_ATTR | 13126 |
| ACL_LIST_ATTR | 13127 |
| POP_MOD_SET_ATTR | 13128 |
| POP_MOD_DEL_ATTR | 13129 |
| POP_MOD_DEL_ATTRVAL | 13130 |
| POP_SHOW_ATTR | 13131 |
| POP_LIST_ATTR | 13132 |
| OBJ_SHOW_ATTRS | 13133 |
| ACL_SHOW_ATTRS | 13134 |
| POP_SHOW_ATTRS | 13135 |
| OBJ_SHOW | 13136 |
| OBJ_LIST | 13137 |
| OBJ_LISTANDSHOW | 13138 |
| **Serververwaltungsbefehle** | |
| SERVER_GET | 13200 |
| SERVER_LIST | 13203 |
| SERVER_PERFORMTASK | 13204 |
| SERVER_GETTASKLIST | 13205 |
| SERVER_REPLICATE | 13206 |
| **Administrator-, Benutzer- und Gruppenverwaltungsbefehle** | |
| ADMIN_SHOWCONF | 13400 |

| USER_CREATE | 13401 |
|---|---|
| USER_IMPORT | 13402 |
| USER_MODDESC | 13403 |
| USER_MODPWD | 13404 |
| USER_MODAUTHMECH | 13405 |
| USER_MODACCVALID | 13406 |
| USER_MODPWDVALID | 13407 |
| USER_DELETE | 13408 |
| USER_SHOWGROUPS | 13409 |
| USER_SHOW | 13410 |
| USER_SHOWDN | 13411 |
| USER_LIST | 13412 |
| USER_LISTDN | 13413 |
| GROUP_CREATE | 13414 |
| GROUP_IMPORT | 13415 |
| GROUP_MODDESC | 13416 |
| GROUP_MODADD | 13417 |
| GROUP_MODREMOVE | 13418 |
| GROUP_DELETE | 13419 |
| GROUP_SHOW | 13420 |
| GROUP_SHOWDN | 13421 |
| GROUP_LIST | 13422 |
| GROUP_LISTDN | 13423 |
| GROUP_SHOWMEMB | 13424 |
| USER_MODGSOUSER | 13425 |
| USER_SET | 13426 |
| GROUP_SET | 13427 |
| **13500 -> 13599 werden von GSO verwendet** | |
| GSO_RESOURCE_CREATE | 13500 |
| GSO_RESOURCE_DELETE | 13501 |
| GSO_RESOURCE_LIST | 13502 |
| GSO_RESOURCE_SHOW | 13503 |

| GSO-Ressourcenberechtigungsbefehle | |
|---|---|
| GSO_RESOURCE_CRED_CREATE | 13504 |
| GSO_RESOURCE_CRED_DELETE | 13505 |
| GSO_RESOURCE_CRED_MODIFY | 13506 |
| GSO_RESOURCE_CRED_LIST | 13507 |
| GSO_RESOURCE_CRED_SHOW | 13508 |
| **GSO-Ressourcengruppenbefehle** | |
| GSO_RESOURCE_GROUP_CREATE | 13509 |
| GSO_RESOURCE_GROUP_DELETE | 13510 |
| GSO_RESOURCE_GROUP_ADD | 13511 |
| GSO_RESOURCE_GROUP_REMOVE | 13512 |
| GSO_RESOURCE_GROUP_LIST | 13513 |
| GSO_RESOURCE_GROUP_SHOW | 13514 |
| **Policy-Befehle** | |
| POLICY_SET_MAX_LOGIN_FAILURES | 13600 |
| POLICY_GET_MAX_LOGIN_FAILURES | 13601 |
| POLICY_SET_DISABLE_TIME_INTERVAL | 13602 |
| POLICY_GET_DISABLE_TIME_INTERVAL | 13603 |
| POLICY_SET_MAX_ACCOUNT_AGE | 13604 |
| POLICY_GET_MAX_ACCOUNT_AGE | 13605 |
| POLICY_SET_ACCOUNT_EXPIRY_DATE | 13606 |
| POLICY_GET_ACCOUNT_EXPIRY_DATE | 13607 |
| POLICY_SET_MAX_INACTIVITY_TIME | 13608 |
| POLICY_GET_MAX_INACTIVITY_TIME | 13609 |
| POLICY_GET_ACCOUNT_CREATION_DATE | 13610 |
| POLICY_GET_LAST_LOGIN_ATTEMPT_DATE | 13611 |
| POLICY_SET_MAX_PASSWORD_AGE | 13612 |
| POLICY_GET_MAX_PASSWORD_AGE | 13613 |
| POLICY_SET_MIN_PASSWORD_AGE | 13614 |
| POLICY_GET_MIN_PASSWORD_AGE | 13615 |
| POLICY_SET_MAX_PASSWORD_REPEATED_CHARS | 13616 |
| POLICY_GET_MAX_PASSWORD_REPEATED_CHARS | 13617 |

| | |
|---|---|
| POLICY_SET_MIN_PASSWORD_ALPHAS | 13618 |
| POLICY_GET_MIN_PASSWORD_ALPHAS | 13619 |
| POLICY_SET_MIN_PASSWORD_NON_ALPHAS | 13620 |
| POLICY_GET_MIN_PASSWORD_NON_ALPHAS | 13621 |
| POLICY_SET_MIN_PASSWORD_DIFFERENT_CHARS | 13622 |
| POLICY_GET_MIN_PASSWORD_DIFFERENT_CHARS | 13623 |
| POLICY_SET_PASSWORD_SPACES | 13624 |
| POLICY_GET_PASSWORD_SPACES | 13625 |
| POLICY_SET_MIN_PASSWORD_LENGTH | 13626 |
| POLICY_GET_MIN_PASSWORD_LENGTH | 13627 |
| POLICY_SET_MIN_PASSWORD_REUSE_TIME | 13628 |
| POLICY_GET_MIN_PASSWORD_REUSE_TIME | 13629 |
| POLICY_GET_PASSWORD_FAILURES | 13630 |
| POLICY_GET_LAST_PASSWORD_CHANGE_DATE | 13631 |
| POLICY_SET_NUMBER_WARN_DAYS | 13632 |
| POLICY_GET_NUMBER_WARN_DAYS | 13633 |
| POLICY_SET_PASSWORD_REUSE_NUM | 13634 |
| POLICY_GET_PASSWORD_REUSE_NUM | 13635 |
| POLICY_SET_TOD_ACCESS | 13636 |
| POLICY_GET_TOD_ACCESS | 13637 |
| **POP-Befehle** | |
| POP_CREATE | 13700 |
| POP_DELETE | 13701 |
| POP_MODIFY | 13702 |
| POP_SHOW | 13703 |
| POP_LIST | 13704 |
| POP_ATTACH | 13705 |
| POP_DETACH | 13706 |
| POP_FIND | 13707 |

| Konfigurationsbefehle 13800 -> 13899 | |
|---|---|
| CFG_CONFIG | 13800 |
| CFG_UNCONFIG | 13801 |
| CFG_REBNEWCERT | 13802 |
| CFG_CHGPORT | 13803 |



# Referenz für Befehl pdadmin

Das Dienstprogramm **pdadmin** ist ein Befehlszeilen-Tool, mit dem Sie die meisten Policy Director-Verwaltungs-Tasks ausführen können. Der Web Portal Manager stellt viele dieser Befehle über seine grafische Benutzerschnittstelle zur Verfügung.

Stichwortindex:

# Einführung in das Dienstprogramm pdadmin

Das Dienstprogramm **pdadmin** ist ein Befehlszeilen-Tool, mit dem Sie die meisten Policy Director-Verwaltungs-Tasks ausführen können. Der Web Portal Manager verfügt über viele der **pdadmin**-Befehle. **pdadmin** bietet jedoch einige erweiterte Verwaltungsfunktionen, die über Web Portal Manager nicht verfügbar sind.

Sie können bestimmte Verwaltungsfunktionen automatisieren, indem Sie Scripts schreiben, die **pdadmin** verwenden. Die Kommunikation zwischen dem Dienstprogramm **pdadmin** und dem Verwaltungsserver (**pdmgrd**) ist über SSL gesichert. Das Dienstprogramm wird als Komponente des PDRTE-Pakets installiert.

## Dienstprogramm pdadmin starten (Befehl login)

- Dialogmodus
- Einzelbefehlszeilenmodus
- Ausführung mehrerer Befehle

### Dialogmodus

Soll **pdadmin** im Dialogmodus gestartet werden, müssen Sie den Befehl **pdadmin** mit einem Befehl **login** und einem Benutzernamen (Administrator) sowie Kennwortoptionen und Argumenten eingeben. Der Administratorbenutzer muss ein registrierter Benutzer in einer LDAP-Registrierungsdatenbank sein.

**UNIX:**

```
# pdadmin
# login –a <Administratorbenutzer> –p <Kennwort>
pdadmin>
```

**Windows:**

```
MSDOS> pdadmin
MSDOS> login –a <Administratorbenutzer> –p <Kennwort>
pdadmin>
```

Geben Sie an der **pdadmin**-Eingabeaufforderung entsprechende Befehle, Optionen und Argumente ein. Schauen Sie in den Befehlsreferenztabellen in diesem Anhang nach.

### Einzelbefehlszeilenmodus

Sie können einen einzelnen Befehl **pdadmin** über die Eingabeaufforderung des Betriebssystems ausführen:

**UNIX:**

```
# pdadmin [–a <Administratorbenutzer>] [–p <Kennwort>] [command]
```

**Windows:**

```
MSDOS> pdadmin [–a <Administratorbenutzer>] [–p <Kennwort>] [command]
```

- Wenn Sie Administratorbenutzer (–a) und Kennwort (–p) angeben, werden Sie als dieser Benutzer angemeldet.
- Wenn Sie Administratorbenutzer (–a) nicht angeben, werden Sie als nicht authentifizierter Benutzer angemeldet.
- Wenn Sie Administratorbenutzer (–a), aber kein Kennwort (–p) angeben, werden Sie zur Kennworteingabe aufgefordert.

Das optionale Befehlsargument gestattet die Ausführung von einmaligen Befehlen. Zum Beispiel wird der Benutzer “test” erstellt, wenn Sie folgenden Befehl eingeben:

```
pdadmin –a sec_master –p pwd user create test
cn=test,ou=austin,o=ibm,c=us test test test1234
```

### Ausführung mehrerer Befehle

Sie können eine spezielle Datei erstellen, die mehrere **pdadmin**-Befehle enthält, die zusammen eine vollständige Task oder eine Reihe von Tasks ausführen. Das Dienstprogramm **pdadmin** akzeptiert ein Dateinamenargument, das die Position einer solchen Datei angibt.

**UNIX:**

```
# pdadmin [–a <Administratorbenutzer>] [–p <Kennwort>] <Dateipfadname>
```

**Windows:**

```
MSDOS> pdadmin [–a <Administratorbenutzer>] [–p <Kennwort>]
<Dateipfadname>
```

## Hilfetext

Geben Sie folgenden Befehl ein, um eine Liste der verfügbaren Befehle aufzurufen:

```
pdadmin> help <Kategorie>
```

Befehlskategorien sind: acl, action, object, server, rsrc, rsrccred, rsrcgroup, admin, login, user, group, policy, pop, errtext.

Informationen zu spezifischer Befehlssyntax können Sie mit folgendem Befehl aufrufen:

```
pdadmin> help <Befehl>
```

## Dienstprogramm pdadmin beenden

Wenn Sie **pdadmin** beenden und zur Eingabeaufforderung zurückkehren wollen, geben Sie den Befehl **exit** oder **quit** ein. Zum Beispiel:

```
pdadmin> exit
```

## Unzulässige Sonderzeichen für GSO-Befehle

Die folgenden Zeichen können Sie für die Erstellung eines GSO-Benutzernamens, eines GSO-Ressourcennamens oder eines GSO-Ressourcengruppennamens nicht verwenden:

```
!"#&()*+,;:<>=@\|
```

Diese Zeichen können Sie zwar für andere LDAP-bezogene Policy Director-Daten (z. B. CN, DN und SN eines Benutzers) verwenden, in der LDAP DN-Syntax und bei den LDAP DN-Filtern haben sie jedoch eine spezielle Bedeutung. Bevor Sie eines dieser Zeichen in Policy Director-Benutzer- und -Gruppennamen verwenden, lesen Sie die Dokumentation zu Ihrem LDAP-Server, um die Auswirkung von Sonderzeichen in LDAP zu bestimmen.

## Benennungseinschränkungen für GSO-Ressourcen

Ressourcen- oder Ressourcenberechtigungsnamen, die Leerzeichen enthalten, müssen zwischen doppelten Anführungszeichen stehen.

# ACL-Befehle

Die folgenden Befehle **pdadmin acl** gestatten die Erstellung von ACL-Policies und erweiterten Attributen.

- ACL-Policy verwalten
- Erweiterte Attribute für ACLs verwalten

## ACL-Policy verwalten

| Befehl | Beschreibung |
|---|---|
| **acl attach <*Objektname*> <*ACL-Name*>** | |
| | Ordnet eine ACL-Policy einem Objekt zu. Ersetzt die ACL, die dem Objekt bereits zugeordnet ist. |
| **acl create <*ACL-Name*>** | |
| | Erstellt eine neue ACL-Policy in der ACL-Datenbank. Beachten Sie, dass dieser Befehl nicht die spezifischen ACL-Einträge erstellt. |
| **acl delete <*ACL-Name*>** | |
| | Löscht eine ACL-Policy aus der ACL-Datenbank. |
| **acl detach <*Objektname*>** | |
| | Gibt die aktuelle ACL-Policy für das angegebene Objekt frei. Beachten Sie, dass dieser Befehl nicht die ACL-Policy aus der ACL-Datenbank löscht. |
| **acl find <*ACL-Name*>** | |
| | Sucht alle Objekte, denen die angegebene ACL-Policy zugeordnet ist, und listet sie auf. |
| **acl list** | |
| | Listet alle ACL-Policies in der ACL-Datenbank auf. |
| **acl modify <*ACL-Name*> description <*Beschreibung*>** | |
| | Entspricht dem Befehl acl modify set description. |
| **acl modify <*ACL-Name*> remove any-other** | |
| | Gestattet das Entfernen des ACL-Eintrags ’Beliebige andere’ aus der angegebenen ACL-Policy-Definition. |
| **acl modify <*ACL-Name*> remove group <*Gruppenname*>** | |
| | Gestattet das Entfernen eines vorhandenen ACL-Eintrags ’Gruppe’ aus der angegebenen ACL-Policy-Definition. |
| **acl modify <*ACL-Name*> remove unauthenticated** | |
| | Gestattet das Entfernen des ACL-Eintrags ’Nicht authentifiziert’ aus der angegebenen ACL-Policy-Definition. |

| Befehl | Beschreibung |
| --- | --- |
| **acl modify <*ACL-Name*> remove user <*Benutzername*>** | |
| | Gestattet das Entfernen eines vorhandenen ACL-Eintrags ’Benutzer’ aus der angegebenen ACL-Policy-Definition. |
| **acl modify <*ACL-Name*> set any-other <*Berechtigungen*>** | |
| | Gestattet das Erstellen und/oder Editieren des ACL-Eintrags ’Beliebige andere’ in der angegebenen ACL-Policy-Definition. Beispiel:<br>`pdadmin> acl modify pubs set any-other r` |
| **acl modify <*ACL-Name*> set description <*Beschreibung*>** | |
| | Gestattet das Erstellen und/oder Editieren des Beschreibungsfelds, das der angegebenen ACL-Policy zugeordnet ist. |
| **acl modify <*ACL-Name*> set group <*Gruppenname*> <*Berechtigungen*>** | |
| | Gestattet das Erstellen und/oder Editieren des ACL-Eintrags ’Gruppe’ in der angegebenen ACL-Policy-Definition. Beispiel:<br>`pdadmin> acl modify pubs set group sales Tr` |
| **acl modify <*ACL-Name*> set unauthenticated <*Berechtigungen*>** | |
| | Gestattet das Erstellen und/oder Editieren des ACL-Eintrags ’Nicht authentifiziert’ in der angegebenen ACL-Policy-Definition. Beispiel:<br>`pdadmin> acl modify docs set unauthenticated r` |
| **acl modify <*ACL-Name*> set user <*Benutzername*> <*Berechtigungen*>** | |
| | Gestattet das Erstellen und/oder Editieren des ACL-Eintrags ’Benutzer’ in der angegebenen ACL-Policy-Definition. Beispiel:<br>`pdadmin> acl modify pubs set user peter Tr` |
| **acl show <*ACL-Name*>** | |
| | Listet alle Einträge, aus denen die Definition der angegebenen ACL-Policy besteht, vollständig auf. |

## Erweiterte Attribute für ACLs verwalten

| Befehl | Beschreibung |
|---|---|
| **acl list <*ACL-Name*> attribute** | |
| | Listet alle erweiterten Attribute auf, die der ACL-Policy zugeordnet sind. |
| **acl modify <*ACL-Name*> delete attribute <*Attributname*>** | |
| | Entfernt das erweiterte Attribut und alle zugehörigen Werte aus der ACL-Policy. |
| **acl modify <*ACL-Name*> delete attribute <*Attributname*> <*Attributwert*>** | |
| | Entfernt den angegebenen Wert aus dem erweiterten Attribut, das der ACL-Policy zugeordnet ist. |
| **acl modify <*ACL-Name*> set attribute <*Attributname*> <*Attributwert*>** | |
| | Fügt ein erweitertes Attribut und seinen Wert einer vorhandenen Zugriffssteuerungsliste (ACL) hinzu. Verwenden Sie diesen Befehl zum Hinzufügen zusätzlicher Werte zu demselben erweiterten Attribut. |
| **acl show <*ACL-Name*> attribute <*Attributname*>** | |
| | Zeigt die Werte des angegebenen erweiterten Attributs, das der ACL-Policy zugeordnet ist, an. |

# Aktionsbefehle

Mit den folgenden Befehlen **pdadmin action** werden zusätzliche Berechtigungsaktionen (ACL-Berechtigungen) und Aktionsgruppen definiert.

- Angepasste ACL-Aktionen erstellen
- Erweiterte ACL-Aktionen und Aktionsgruppen erstellen

## Angepasste ACL-Aktionen erstellen

| Befehl | Beschreibung |
|---|---|
| **action create <*Aktionsname*> <*Aktionsbezeichnung*> <*Aktionsart*>** | |
| | Definiert eine neue Policy Director-Berechtigungsaktion (Berechtigung). Erstellt ein neues Berechtigungszeichen, das diese Aktion auf der Management Console darstellt. Das Argument **Aktionsname** gibt den Namen der neuen, aus einem Zeichen bestehenden Berechtigung an. Das Argument **Aktionsbezeichnung** gibt die Bezeichnung für das neue Markierungsfeld an, das in der Management Console angezeigt wird. Das Argument **Aktionsart** gibt eine organisatorische Kategorie (Art) an, wo diese Berechtigung in der Management Console-Anzeige (ACL-Indexzunge) erscheint. Beispiel:<br>`pdadmin> action create k time Ext-Authzn` |
| **action delete <*Aktionsname*>** | |
| | Löscht eine vorhandene, durch den Befehl **action create** erstellte Berechtigungsaktion. Beispiel:<br>`pdadmin> action delete k` |
| **action list** | |
| | Listet alle vorhandenen ACL-Aktionen (Berechtigungen) in folgendem Format auf: **Aktionsname Aktionsbezeichnung Aktionsart**. Beispiel:<br>`r read WebSEAL`<br>`...` |

# Erweiterte ACL-Aktionen und Aktionsgruppen erstellen

| Befehl | Beschreibung |
|---|---|
| **action create <*Aktionsname*> <*Aktionsbezeichnung*> <*Aktionsart*> <*Aktionsgruppenname*>** | |
| | Eine neue ACL-Aktionsdefinition für die angegebene Aktionsgruppe erstellen. |
| **action delete <*Aktionsname*> <*Aktionsgruppenname*>** | |
| | Eine ACL-Aktionsdefinition aus der angegebenen Aktionsgruppe löschen. |
| **action group list** | |
| | Listet alle ACL-Aktionsgruppennamen auf. |
| **action group create <*Aktionsgruppenname*>** | |
| | Neue ACL-Aktionsgruppe erstellen. |
| **action group delete <*Aktionsgruppenname*>** | |
| | ACL-Aktionsgruppe löschen. |
| **action list <*Aktionsgruppenname*>** | |
| | Alle ACL-Aktionsdefinitionen für die angegebene Aktionsgruppe auflisten. |

# Objektbefehle

Mit den Befehlen **pdadmin object** und **objectspace** können zusätzliche Objektbereiche mit geschützten Objekten, die von Anwendungen anderer Hersteller verwendet werden, erstellt werden.

- Angepassten Objektbereich verwalten
- Geschützte Objekte verwalten
- Erweiterte Attribute für geschützte Objekte verwalten

## Angepassten Objektbereich verwalten

| Befehl | Beschreibung |
|---|---|
| **objectspace create <*Objektbereichsname*> <*Beschreibung*> <*Art*>** | |
| | Erstellt einen neuen geschützten Objektbereich, in den geschützte Objekte gestellt werden können. |
| **objectspace delete <*Objektbereichsname*>** | |
| | Löscht einen vorhandenen geschützten Objektbereich und alle zugeordneten geschützten Objekte. |
| **objectspace list** | |
| | Listet alle geschützten Objektbereiche auf. |

## Geschützte Objekte verwalten

| Befehl | Beschreibung |
|---|---|
| **object create <*Objektname*> <*Beschreibung*> <*Art*> ispolicyattachable {yes\|no}** | |
| | Erstellt ein neues geschütztes Objekt. Das Argument **Objektname** ist der Name für das erstellte Objekt. Dieser Name muss eindeutig sein. Das Argument **Beschreibung** ist eine beliebige Zeichenfolge, die das Objekt beschreibt. Diese Informationen erscheinen im Befehl **object show**. Das Argument **Art** gibt das Grafiksymbol an, das diesem Objekt zugeordnet ist und von der Management Console angezeigt wird. Die Arten liegen im Bereich von 0-13. Die Arten 10 und 13 sind beispielsweise für Containerobjekte geeignet. Das Argument **ispolicyattachable** legt fest, ob Sie diesem Objekt eine ACL-Policy zuordnen können. Ein Beispiel finden Sie in „Gruppencontainerobjekte erstellen” auf Seite 122. |
| **object delete <*Objektname*>** | |
| | Löscht ein geschütztes Objekt. |
| **object list <*Objektname*>** | |
| | Neu: Listet alle Kindobjekte auf, die unter dem angegebenen geschützten Objekt gruppiert sind. Alt: Listet die Objekte auf, die unter dem angegebenen Verzeichnis gruppiert sind, und zeigt die Namen aller ACLs an, die den einzelnen Objekten zugeordnet sind. Beachten Sie, dass dieser Befehl die Baumstruktur nicht über dieses Verzeichnis hinaus erweitert. |
| **object listandshow <*Objektname*>** | |
| | Listet alle Kindobjekte auf, die unter dem angegebenen geschützten Objekt gruppiert sind, und zeigt alle Werte an, die diesen Objekten zugeordnet sind. |

| Befehl | Beschreibung |
|---|---|
| **object modify <*Objektname*> set name <*neuer-Objektname*>** | |
| | Benennt das geschützte Objekt oder den geschützten Objektbereich um. |
| **object modify <*Objektname*> set description <*Beschreibung*>** | |
| | Ändert die Beschreibung des geschützten Objekts oder des geschützten Objektbereichs. |
| **object modify <*Objektname*> set type <*Art*>** | |
| | Ändert die Art des geschützten Objekts oder des geschützten Objektbereichs. |
| **object modify <*Objektname*> set ispolicyattachable {yes\|no}** | |
| | Ändert die Angabe, ob dem geschützten Objekt eine POP-Policy zugeordnet werden darf. |
| **object show <*Objektname*>** | |
| | Neu: Zeigt alle Werte, die einem geschützten Objekt zugeordnet sind. Alt: Zeigt den Objektnamen und den Namen jeder ihm zugeordneten Zugriffssteuerungsliste (ACL) an. Ist keine ACL zugeordnet, wird “Keine ACL” angezeigt. |

# Erweiterte Attribute für geschützte Objekte verwalten

| Befehl | Beschreibung |
|---|---|
| **object list <*Objektname*> attribute** | |
| | Listet alle erweiterten Attribute auf, die dem geschützten Objekt zugeordnet sind. |
| **object modify <*Objektname*> delete attribute <*Attributname*>** | |
| | Entfernt das angegebene erweiterte Attribut und alle zugehörigen Werte aus dem angegebenen geschützten Objekt. |
| **object modify <*Objektname*> delete attribute <*Attributname*> <*Attribut-wert*>** | |
| | Entfernt den angegebenen Wert aus dem erweiterten Attribut, das dem angegebenen geschützten Objekt zugeordnet ist. |
| **object modify <*Objektname*> set attribute <*Attributname*> <*Attribut-wert*>** | |
| | Fügt das erweiterte Attribut und seinen Wert einem geschützten Objekt hinzu. |
| **object show <*Objektname*> attribute <*Attributname*>** | |
| | Zeigt die Werte des angegebenen erweiterten Attributs, das dem geschützten Objekt zugeordnet ist, an. |

# Befehle für Policy für geschützte Objekte (POP)

Mit den Befehlen **pdadmin pop** können Policies für geschützte Objekte (Protected Object Policies, POP) und erweiterte Attribute für POP-Policies erstellt werden.

- POP-Policies verwalten
- Erweiterte Attribute für POP-Policies verwalten

## POP-Policies verwalten

<table>
<tr><th>Befehl</th><th>Beschreibung</th></tr>
<tr><td colspan="2"><b>pop attach <<i>Objektname</i>> <<i>POP-Name</i>></b></td></tr>
<tr><td></td><td>Eine POP-Policy einem geschützten Objekt zuordnen.</td></tr>
<tr><td colspan="2"><b>pop create <<i>POP-Name</i>></b></td></tr>
<tr><td></td><td>POP-Policy erstellen.</td></tr>
<tr><td colspan="2"><b>pop delete <<i>POP-Name</i>></b></td></tr>
<tr><td></td><td>POP-Policy löschen.</td></tr>
<tr><td colspan="2"><b>pop detach <<i>Objektname</i>></b></td></tr>
<tr><td></td><td>POP-Policy bei einem geschützten Objekt freigeben.</td></tr>
<tr><td colspan="2"><b>pop find <<i>POP-Name</i>></b></td></tr>
<tr><td></td><td>Alle geschützten Objekte, denen POP-Policies zugeordnet sind, suchen und auflisten.</td></tr>
<tr><td colspan="2">pop list</td></tr>
<tr><td></td><td>Alle erstellten POP-Policies auflisten.</td></tr>
<tr><td colspan="2"><b>pop modify <<i>POP-Name</i>> set audit-level {all|none|<<i>Prüfungsstufenliste</i>>}</b></td></tr>
<tr><td></td><td>Prüfungsstufe für POP-Policy ändern. Bei der Prüfungsstufenliste kann es sich um eine Liste mit Kommatrennzeichen und folgenden Angaben handeln: Zulassen, Verweigern, Fehler, Admin.</td></tr>
<tr><td colspan="2"><b>pop modify <<i>POP-Name</i>> set description <<i>Beschreibung</i>></b></td></tr>
<tr><td></td><td>Beschreibung der POP-Policy ändern.</td></tr>
</table>

<table>
<tr><th>Befehl</th><th>Beschreibung</th></tr>
<tr><td colspan="2">**pop modify <*POP-Name*> set ipauth add <*Netz*> <*Netzmaske*> <*Authentifizierungsstufe*>**</td></tr>
<tr><td></td><td>IP-Authentifizierungszugriff der POP-Policy ändern.</td></tr>
<tr><td colspan="2">**pop modify <*POP-Name*> set ipauth anyothernw <*Authentifizierungsstufe*>**</td></tr>
<tr><td></td><td>IP-Authentifizierungszugriff der POP-Policy ändern.</td></tr>
<tr><td colspan="2">**pop modify <*POP-Name*> set ipauth remove <*Netz*> <*Netzmaske*>**</td></tr>
<tr><td></td><td>IP-Authentifizierungszugriff der POP-Policy ändern.</td></tr>
<tr><td colspan="2">**pop modify <POP-Name> set qop {none|integrity|privacy}**</td></tr>
<tr><td></td><td>Sicherungsstufe der POP-Policy ändern.</td></tr>
<tr><td colspan="2">**pop modify <*POP-Name*> set tod-access <*Zugriffszeit*>**</td></tr>
<tr><td></td><td>Zugriffszeit der POP-Policy ändern. Das Argument ’Zugriffszeit’ hat folgendes Format: <{anyday|weekday|<*Tagesliste*>}>: <{anytime|<*Zeitspezifikation*>-<*Zeitspezifikation*>}> [:{utc|local}]. Gültige Werte für die Variable ’Tagesliste’ sind Mon, Die, Mit, Don, Fre, Sam, Son. Die Bereichsvariable ’Zeitspezifikation’ muss wie folgt ausgedrückt werden: hhmm. Zum Beispiel: 0700-1945. Die optionale Zeitzone ist standardmäßig ’lokal’.</td></tr>
<tr><td colspan="2">**pop modify <*POP-Name*> set warning {on|off}**</td></tr>
<tr><td></td><td>Warnungsanzeiger der POP-Policy ändern.</td></tr>
<tr><td colspan="2">**pop show <*POP-Name*>**</td></tr>
<tr><td></td><td>Details der POP-Policy anzeigen.</td></tr>
</table>

## Erweiterte Attribute für POP-Policies verwalten

| Befehl | Beschreibung |
|---|---|
| **pop list <*POP-Name*> attribute** | |
| | Listet alle erweiterten Attribute auf, die einer POP-Policy zugeordnet sind. |
| **pop modify <*POP-Name*> delete attribute <*Attributname*>** | |
| | Entfernt das angegebene erweiterte Attribut und alle zugehörigen Werte aus der angegebenen POP-Policy. |
| **pop modify <*POP-Name*> delete attribute <*Attributname*> <*Attributwert*>** | |
| | Entfernt den angegebenen Wert aus dem erweiterten Attribut, das der angegebenen POP-Policy zugeordnet ist. |
| **pop modify <*POP-Name*> set attribute <*Attributname*> <*Attributwert*>** | |
| | Fügt das erweiterte Attribut und seinen Wert einer POP-Policy hinzu. |
| **pop show <*POP-Name*> attribute** <***Attributname***> | |
| | Details bestimmter POP-Attribute anzeigen. |

## Serverbefehle

Die folgenden Befehle **pdadmin server** sind geeignet für Verwaltungs-Tasks auf den Policy Director-Servern.

Das Argument *Servername* wird als tatsächlicher Maschinenname und die von diesem Befehl verwendete Policy Director-Komponente ausgedrückt. Die Policy Director-Komponente kann ein Basisserver (z. B. **pdmgrd** oder **pdacld**), ein Policy Director-Ressourcenmanager (z. B. **webseald**) oder ein externer Anwendungsserver sein:

```
<Policy-Director-Komponente>-<Maschinenname>
```

Wenn der Maschinenname beispielsweise **cruz** lautet und die Policy Director-Komponente WebSEAL ist, lautet der *Servername*:

```
webseald-cruz
```

| Befehl | Beschreibung |
|---|---|
| **server list** | |
| | Listet alle registrierten Server auf. Verwenden Sie das durch diesen Befehl angezeigte Servernamensformat für alle Argumente <*Servername*>. |
| **server listtasks <*Servername*>** | |
| | Ruft die für diesen Server verfügbare Liste der Tasks (Befehle) ab. |
| **server replicate [–server <*Servername*>]** | |
| | |
| **server show <*Servername*>** | |
| | Zeigt die Merkmale des angegebenen Servers an. |
| **server task <*Servername*> <*Befehl*>** | |
| | Sendet den angegebenen Befehl an den angegebenen Server. |

## Technische Anmerkungen

Achten Sie darauf, dass das Argument *Servername* in genau demselben Format eingegeben werden muss, das in der Ausgabe des Befehls **pdadmin server list** angezeigt wird.

Das Argument *Servername* ist der vollständige Ausdruck des tatsächlichen Maschinennamens und der von diesem Befehl verwendeten Policy Director-Komponente (z. B. WebSEAL).

```
<Policy-Director-Komponente>-<Maschinenname>
```

Wenn der Maschinenname beispielsweise **cruz** lautet und die Policy Director-Komponente WebSEAL ist, lautet der *Servername*:

```
webseald-cruz
```

Prüfen Sie mit dem Befehl **server list** die *Servernamen*ausdrücke:

```
pdadmin> server list
webseald-cruz
```

Sollen die Merkmale des WebSEAL-Servers auf der Maschine **cruz** angezeigt werden, geben Sie folgendes ein:

```
pdadmin> server show webseald-cruz
webseald-cruz
    Beschreibung: webseald/cruz
    Host-Name: cruz
    Principal: webseald/cruz
    Port: 7234
    Für Hinweise zur Aktualisierung der Berechtigungsdatenbank
    empfangsbereit: ja
    AZN-Verwaltungsservice:
        webseal-admin-svc
        azn_admin_svc_trace
```

## Verwaltungsinformationsbefehl

Der folgende Verwaltungsbefehl zeigt Informationen zum Server an.

| Befehl | Beschreibung |
|---|---|
| **admin show configuration** | |
| | Zeigt aktuelle Serverkonfigurationsdaten an, z. B.:<br>■ ob die Benutzerregistrierungsdatenbank in LDAP enthalten ist<br>■ ob GSO aktiviert ist oder nicht<br>Beispiel:<br>`pdadmin> admin show configuration`<br>Dieser Befehl hat etwa folgende Ausgabe:<br>`LDAP: TRUE`<br>`SECAUTHORITY: Default`<br>`GSO: TRUE` |

## Benutzerverwaltungsbefehle

Die folgenden Befehle **pdadmin user** steuern Benutzereinträge in der LDAP-Registrierungsdatenbank.

Ein **Benutzer** ist ein registriertes Mitglied der gesicherten Domäne von Policy Director. Ein **GSO-Benutzer** ist ein Policy Director-Benutzer, der die zusätzliche Berechtigung für die Arbeit mit Webressourcen, z. B. ein Webserver, besitzt.

| Befehl | Beschreibung |
|---|---|
| **user create [–gsouser] [–no-password-policy] <*Benutzername*> <*DN*> <*CN*> <*SN*> <*Kennwort*> [*Gruppenname*]** | |
| | Erstellt ein neues Policy Director-Benutzerkonto (**secUser**) in der LDAP-Benutzerregistrierungs-datenbank. Der registrierte Name (Distinguished Name, DN) muss bekannt sein, damit Sie ein neues Benutzer-konto erstellen können.<br><br>Wenn das optionale Argument **-gsouser** angegeben wird, wird der Benutzer außerdem zu einem GSO-Benutzer (**gsoUser**).<br><br>Das Argument **Benutzername** ist der Name des erstell-ten Benutzers. Dieser Name muss eindeutig sein.<br><br>Das Argument **DN** ist der registrierte LDAP-Name, der dem erstellten Benutzer zugeordnet wird. Beispiel:<br>`"cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US"`<br><br>Der DN muss eindeutig sein.<br><br>Das Argument **CN** ist der allgemeine Name (common name), der dem erstellten Benutzer zugeordnet wird. Beispiel:<br>`Diana Lucas`<br><br>Das Argument **SN** ist der Familienname (surname) des erstellten Benutzers. Beispiel:<br>`Lucas`<br><br>Das Argument **Kennwort** ist das Kennwort, das Sie für diesen neuen Benutzer definieren. Kennwörter müssen den Kennwort-Policies entsprechen, die der Policy Director-Administrator festlegt. Beispiel:<br>`mypasswd`<br><br>Das optionale Argument **Gruppenname** ordnet den Benutzer einer Anfangsgruppe zu. *Fortsetzung...* |

| Befehl | Beschreibung |
| --- | --- |
| | Beispiel (in einer Zeile eingegeben):<br>`pdadmin> user create –gsouser dlucas "cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US" "Diana Lucas" Lucas` *`mypasswd`*<br><br>Damit dieses Benutzerkonto gültig wird, müssen Sie diesen Benutzer manuell aktivieren, indem Sie die Benutzerinformationen ändern. Um die Informationen ändern zu können, müssen Sie für die Markierung **account-valid** “yes” angeben. Soll eine Beschreibung für einen Benutzer hinzugefügt werden, müssen Sie mit dem Befehl **modify user** die Benutzerkonto-informationen ändern. |
| **user import [–gsouser] <*Benutzername*> <*DN*> [*Gruppenname*]** | |
| | Kopiert die Informationen zu einem Benutzer aus dem LDAP-Verzeichnis. Mit diesem Befehl kann ein vorhandener Benutzer (dessen DN in der LDAP-Datenbank bereits vorhanden ist) durch Policy Director-Informationen aktualisiert werden, so dass der Benutzer Mitglied der gesicherten Domäne werden kann. Das optionale Argument **Gruppenname** ordnet den Benutzer einer Anfangsgruppe zu. Beispiel (in einer Zeile eingegeben):<br>`pdadmin> user import –gsouser mlucaser "cn=Mike Lucaser,ou=Austin,o=Wesley Inc,c=US"` |
| **user modify <*Benutzername*> description <*Beschreibung*>** | |
| | Fügt eine Beschreibung hinzu, die Informationen zur Verfügung stellt, die dem Administrator das Identifizieren dieses Benutzers erleichtern. Beispiel (in einer Zeile eingegeben):<br>`pdadmin> user modify dlucas description "Diana Lucas, Kreditabt. HCUS"` |
| **user modify <*Benutzername*> password <*Kennwort*>** | |
| | Ersetzt das aktuelle Kennwort des Benutzers durch ein neues Kennwort. Für diese Operation gibt es keine Kennwortbestätigung. Beispiel:<br>`pdadmin> user modify dlucas password newpasswd` |

| Befehl | Beschreibung |
|---|---|
| **user modify <*Benutzername*> authentication-mechanism <*Mechanismus*>** | |
| | Ändert das für die Authentifizierung verwendete Verfahren. Wenn kein DN angegeben ist, ist das erste Auftreten von **Benutzername** das Benutzerkonto, das geändert wird. Beispiel (in einer Zeile eingegeben):<br>`pdadmin> user modify dlucas Berechtigungsmechanismus, Standardwert: LDAP` |
| **user modify <*Benutzername*> account-valid {yes\|no}** | |
| | Gibt an, ob ein Konto aktiv oder inaktiv ist. Zum Aktivieren des Kontos wählen Sie “yes” aus, zum Inaktivieren “no”. Beispiel:<br>`pdadmin> user modify dlucas account-valid yes` |
| **user modify <*Benutzername*> password-valid {yes\|no}** | |
| | Gibt an, ob ein Kennwort aktiv oder inaktiv ist. Wird hier “no” angegeben, ist der Benutzer gezwungen, das Kennwort bei der nächsten Anmeldung zu ändern. Beispiel:<br>`pdadmin> user modify dlucas password-valid no` |
| **user modify <*Benutzername*> gsouser {yes\|no}** | |
| | Gibt an, ob der angegebene Policy Director-Benutzer auch ein GSO-Benutzer ist. Wählen Sie “yes” aus, um den Benutzer als GSO-Benutzer hinzuzufügen; wählen Sie “no” aus, um den Benutzer als GSO-Benutzer zu entfernen. Beispiel:<br>`pdadmin> user modify dlucas gsouser no` |

<table>
<tr><th>Befehl</th><th>Beschreibung</th></tr>
<tr><td colspan="2"><b>user delete <<i>Benutzername</i>></b></td></tr>
<tr><td></td><td>Löscht ein vorhandenes Benutzerkonto aus der LDAP-Benutzerregistrierungsdatenbank. Beim Löschen eines Policy Director-Benutzerkontos werden auch die GSO-Benutzerkontoinformationen aus der LDAP-Registrierungsdatenbank gelöscht. Beispiel:<br><code>pdadmin> user delete dlucas</code><br><br>Alle Ressourcenberechtigungen, die einem Benutzerkonto zugeordnet sind, werden automatisch gleichzeitig mit dem Löschen des Benutzerkontos entfernt.</td></tr>
<tr><td colspan="2"><b>user show <<i>Benutzername</i>></b></td></tr>
<tr><td></td><td>Zeigt die Benutzerkontoinformationen für den angegebenen Benutzer an. Beispiel:<br><code>pdadmin> user show dlucas</code><br><br>Dieser Befehl hat etwa folgende Ausgabe:<br><code>Anmelde-ID: dlucas</code><br><code>LDAP-DN: cn=Diana Lucas,ou=Austin,o=Wesley Inc,c=US</code><br><code>LDAP-CN: Diana Lucas</code><br><code>LDAP-SN: Lucas</code><br><code>Beschreibung: Diana Lucas, Kreditabt. HCUS</code><br><code>Ist SecUser: true</code><br><code>Ist GSO-Benutzer: false</code><br><code>Konto gültig: true</code><br><code>Kennwort gültig: true</code><br><code>Berechtigungsmechanismus: Default:LDAP</code></td></tr>
</table>

| Befehl | Beschreibung |
|---|---|
| **user show-dn <*DN*>** | |
| | Liefert zusätzliche Informationen zu dem Benutzer, wenn Sie den registrierten Namen (Distinguished Name, DN) angeben.<br><br>Beispiel (in einer Zeile eingegeben):<br><br>`pdadmin> user show-dn "cn=Diana`<br>`Lucas,ou=Austin,o=Wesley Inc,c=US"`<br><br>Dieser Befehl hat etwa folgende Ausgabe:<br><br>`Anmelde-ID: dlucas`<br>`LDAP-DN: cn=Diana Lucas,ou=Austin,o=Wesley`<br>`Inc,c=US`<br>`LDAP-CN: Diana Lucas`<br>`LDAP-SN: Lucas`<br>`Beschreibung: Diana Lucas, Kreditabt. HCUS`<br>`Ist SecUser: true`<br>`Ist GSO-Benutzer: false`<br>`Konto gültig: true`<br>`Kennwort gültig: true`<br>`Berechtigungsmechanismus: Default:LDAP` |

| Befehl | Beschreibung |
|---|---|
| **user show-groups <*Benutzername*>** | |
| | Zeigt die Gruppen an, in denen der angegebene Benutzer ein Mitglied ist. Beispiel:<br>`pdadmin> user show-groups dlucas`<br><br>Dieser Befehl hat etwa folgende Ausgabe:<br>`Verkauf`<br>`Kredit`<br>`Technik` |
| **user list <*Muster*> <*max.-Zurückgabe*>** | |
| | Generiert eine Liste aller konfigurierten Benutzerkonten (nach Benutzernamen) für das angegebene Muster. Die Listeneinträge werden in der Reihenfolge der Erstellung der Benutzerkonten angezeigt. Mit dem Argument **Muster** können Sie ein Muster für den Principal-Namen angeben. Das Muster kann eine Mischung aus Platzhalterzeichen und Zeichenfolgekonstanten enthalten, und die Groß-/Kleinschreibung muss beachtet werden (z. B. *luca*). Das Argument **max.-Zurückgabe** begrenzt die Anzahl der gesuchten und zurückgegebenen Einträge für eine einzelne Anforderung (z. B. 2). Beachten Sie, dass die zurückgegebene Anzahl auch durch die LDAP-Serverkonfiguration bestimmt wird, in der die maximale Anzahl der Ergebnisse, die bei einer Suchoperation zurückgegeben werden kann, festgelegt ist. Die tatsächlich zurückgegebene Anzahl an Einträgen ist das Minimum von <max.-Zurückgabe> und dem konfigurierten Wert im LDAP-Server. Beispiel:<br>`pdadmin> user list *luca* 2`<br><br>Dieser Befehl hat etwa folgende Ausgabe:<br>`dlucas`<br>`mlucaser` |

| Befehl | Beschreibung |
|---|---|
| **user list-dn <*Muster*> <*max.-Zurückgabe*>** | |
| | Wenn der registrierte Name (DN) nur teilweise bekannt ist, wird eine Liste aller konfigurierten Benutzerkonten nach registrierten Namen generiert. Die Listeneinträge werden in der Reihenfolge der Erstellung der Benutzernamen angezeigt. Einzelheiten zu den Befehlsargumenten finden Sie beim Befehl **user list** oben. Mit dem Argument **Muster** können Sie ein Muster für den Abschnitt mit dem allgemeinen Namen (Common Name, CN) des registrierten Namens des Benutzers (ohne Komponente “cn=”) angeben. Beispiel:<br>`pdadmin> user list-dn *luca* 2`<br><br>Dieser Befehl hat etwa folgende Ausgabe:<br>`cn=Diana Lucas,ou=Austin,o=Wesley, Inc,c=US`<br>`cn=Mike Lucaser,ou=Austin,o=Wesley, Inc,c=US` |
| **user list-gsouser <*Muster*> <*max.-Zurückgabe*>** | |
| | Generiert eine Liste, die nur die GSO-Benutzer enthält und nach registrierten Namen angezeigt wird. Die Listeneinträge werden in der Reihenfolge der Erstellung der GSO-Benutzer angezeigt. Einzelheiten zu den Befehlsargumenten finden Sie beim Befehl **user list** oben. Beispiel:<br>`pdadmin> user list-gsouser *luca* 2`<br><br>Dieser Befehl hat etwa folgende Ausgabe:<br>`cn=Diana Lucas,ou=Austin,o=Wesley, Inc,c=US`<br>`cn=Mike Lucaser,ou=Austin,o=Wesley, Inc,c=US` |

# Gruppenverwaltungsbefehle

Die folgenden Befehle **pdadmin group** steuern Gruppeneinträge in der LDAP-Verzeichnisregistrierungsdatenbank.

Eine **Gruppe** ist eine Reihe von Policy Director-Benutzerkonten mit ähnlichen Attributen. Mit Hilfe von Gruppen können Sie einen Gruppennamen in einer Zugriffssteuerungsliste (Access Control List, ACL) angeben, so dass Sie nicht alle Benutzer einzeln auflisten müssen.

| Befehl | Beschreibung |
|---|---|
| **group create <*Gruppenname*> <*DN*> <*CN*> [*Gruppencontainerobjekt*]** | |
| | Erstellt eine neue Policy Director-Gruppe (ISSecGroup) in der LDAP-Benutzerregistrierungsdatenbank. Das Argument **Gruppenname** ist der Name der erstellten Gruppe. Dieser Name muss eindeutig sein. Das Argument **DN** ist der registrierte LDAP-Name, der der erstellten Zugriffsgruppe zugeordnet wird. Beispiel:<br>`"cn=credit,ou=Austin,o=Wesley Inc,c=US")`<br><br>Das Argument **CN** ist der allgemeine Name, der der Gruppe zugeordnet wird. Beispiel:<br>`Kredit`<br><br>Das optionale Argument **Gruppencontainerobjekt** ordnet die Gruppe dem angegebenen Gruppencontainer zu. Wenn Sie dieses Argument nicht verwenden, wird die Gruppe standardmäßig in den Objektbereich unter /Management/Groups gestellt. Beispiel (in einer Zeile eingegeben):<br>`pdadmin> group create credit`<br>`"cn=credit,ou=Austin,o=Wesley Inc,c=US" Credit` |

| Befehl | Beschreibung |
|---|---|
| **group import <*Gruppenname*> <*DN*> [*Gruppencontainerobjekt*]** | |
| | Importiert die Informationen zu einer vorhandenen LDAP-Registrierungsdatenbankgruppe, um eine Policy Director-Gruppe zu erstellen. Die Gruppe muss in der LDAP-Registrierungsdatenbank bereits vorhanden sein, bevor Sie die Informationen importieren und eine Policy Director-Gruppe erstellen können. Der Name der erstellten Gruppe muss in dem Objektbereich eindeutig sein. Wird kein Gruppencontainerobjekt angegeben, wird die Gruppe in /Management/Groups aufgenommen. Beispiel (in einer Zeile eingegeben):<br>`pdadmin> group import engineering`<br>`"cn=engineering,ou=Austin,o=Wesley Inc,c=US"` |
| **group modify <*Gruppenname*> description <*Beschreibung*>** | |
| | Fügt eine Beschreibung für die angegebene Gruppe hinzu, durch die sie der IntraVers-Administrator besser identifizieren kann. Beispiel (in einer Zeile eingegeben):<br>`pdadmin> group modify credit description`<br>`"Kredit, Abt. HCUS"` |
| **group modify <*Gruppenname*> add <*Benutzername*>** | |
| | Fügt der angegebenen Gruppe einen neuen Benutzer hinzu. Beispiel:<br>`pdadmin> group modify engineering add dlucas` |
| **group modify <*Gruppenname*> remove <*Benutzername*>** | |
| | Löscht einen vorhandenen Benutzer aus der angegebenen Gruppe. Beispiel:<br>`pdadmin> group modify engineering remove dlucas` |
| **group delete <*Gruppenname*>** | |
| | Löscht eine vorhandene Gruppe und alle Einträge, die der Gruppe zugeordnet sind. Beispiel:<br>`pdadmin> group delete engineering` |

| Befehl | Beschreibung |
|---|---|
| **group show <*Gruppenname*>** | |
| | Zeigt die Details zu einer angegebenen Gruppe an. Beispiel:<br>`pdadmin> group show credit`<br><br>Dieser Befehl hat etwa folgende Ausgabe:<br>`Gruppen-ID: credit`<br>`LDAP-DN: cn=credit,ou=Austin,o=Wesley Inc,c=US`<br>`Beschreibung: Kredit, Abt. HCUS`<br>`LDAP-CN: credit`<br>`Ist SecGroup: true` |
| **group show-dn <*DN*>** | |
| | Liefert den Gruppennamen für den angegebenen registrierten Namen (Distinguished Name, DN). Beispiel (in einer Zeile eingegeben):<br>`pdadmin> group show-dn`<br>`cn=credit,ou=Austin,o=Wesley Inc,c=US`<br><br>Dieser Befehl hat etwa folgende Ausgabe:<br>`Gruppen-ID: credit`<br>`LDAP-DN: cn=credit,ou=Austin,o=Wesley Inc,c=US`<br>`Beschreibung: Kredit, Abt. HCUS`<br>`LDAP-CN: credit`<br>`Ist SecGroup: true` |
| **group show-members <*Gruppenname*>** | |
| | Zeigt die Mitglieder der angegebenen Gruppe nach registrierten Namen an. Beispiel:<br>`pdadmin> group show-members credit`<br><br>Dieser Befehl hat etwa folgende Ausgabe:<br>`dlucas`<br>`mlucaser` |

| Befehl | Beschreibung |
|---|---|
| **group list <Muster> <max.-Zurückgabe>** | |
| | Generiert eine Liste (nach Gruppennamen) aller konfigurierten Gruppen, deren Namen dem angegebenen Muster entsprechen. Mit dem Argument **Muster** können Sie ein Muster für den Gruppennamen angeben. Das Muster kann eine Mischung aus Platzhalterzeichen und Zeichenfolgekonstanten enthalten, und die Groß-/Kleinschreibung muss beachtet werden (z. B. *austin*). Das Argument **max.-Zurückgabe** begrenzt die Anzahl der gesuchten und zurückgegebenen Einträge für eine einzelne Anforderung (z. B. 2). Beachten Sie, dass die zurückgegebene Anzahl auch durch die LDAP-Serverkonfiguration bestimmt wird, in der die maximale Anzahl der Ergebnisse, die bei einer Suchoperation zurückgegeben werden kann, festgelegt ist. Die tatsächlich zurückgegebene Anzahl an Einträgen ist das Minimum von <max.-Zurückgabe> und dem konfigurierten Wert im LDAP-Server. Beispiel:<br>`pdadmin> group list *a* 2`<br><br>Dieser Befehl hat etwa folgende Ausgabe:<br>`Verkauf`<br>`Marketing` |
| **group list-dn <*Muster*> <*max.-Zurückgabe*>** | |
| | Wenn der registrierte Name (DN) teilweise bekannt ist, wird eine Liste aller konfigurierten Gruppen nach registrierten Namen für das angegebene Muster generiert. Einzelheiten zu den Befehlsargumenten finden Sie beim Befehl **group list** oben. Mit dem Argument **Muster** können Sie ein Muster für den Abschnitt mit dem allgemeinen Namen (Common Name, CN) des registrierten Namens der Gruppe (ohne Komponente “cn=”) angeben.<br>`pdadmin> group list-dn *t* 2`<br><br>Dieser Befehl hat etwa folgende Ausgabe:<br>`cn=credit,ou=Austin,o=Wesley Inc,c=US sales`<br>`cn=marketing,ou=Boston,o=Austin Sale,c=US marketing` |

# Ressourcenverwaltungsbefehle

Die folgenden Befehle **pdadmin** steuern ressourcenbezogene Informationen.

Zu den ressourcenbezogenen Informationen gehören:

- Ressourcen verwalten
- Ressourcengruppen verwalten
- Ressourcenberechtigungen verwalten

## Ressourcen verwalten

Mit den folgenden Befehlen **pdadmin rsrc** können Sie verschiedene Ressourcen verwalten, z. B. Webserver für GSO-Benutzer.

Eine Ressource ist ein Webserver. Die Kennung **–T** in einer WebSEAL-Junction-Definition identifiziert den Webserver.

Ein Befehl **pdadmin rsrc** identifiziert den Namen der Webressource.

| Befehl | Beschreibung |
|---|---|
| **rsrc create <*Ressourcenname*> [–desc <*Beschreibung*>]** | |
| | Erstellt und benennt einen Webserver als Ressource. Das Argument **Ressourcenname** ist der Name, den die Webressource zum Identifizieren erhält. Beispiel:<br>`engwebs01`<br><br>Das optionale Argument **Beschreibung** kann hinzugefügt werden, um dem Administrator das Identifizieren dieser Ressource zu erleichtern. Allen optionalen Parametern muss ein Bindestrich (–) vorangestellt werden. Beschreibungen, die Leerzeichen enthalten, müssen zwischen doppelten Anführungszeichen (“) stehen. Beispiel (in einer Zeile eingegeben):<br>`pdadmin> rsrc create engwebs01 –desc`<br>`"Technischer Webserver – Raum 4807"` |

| Befehl | Beschreibung |
|---|---|
| **rsrc delete <*Ressourcenname*>** | |
| | Löscht die angegebene Ressource, einschließlich der Beschreibung. Die Ressource muss vorhanden sein; ansonsten wird ein Fehler angezeigt. Beispiel:<br>`pdadmin> rsrc delete engwebs01` |
| **rsrc list** | |
| | Zeigt die Namen aller Webressourcen (nach Ressourcennamen), die im LDAP-Verzeichnis definiert sind, an. Beispiel:<br>`pdadmin> rsrc list`<br><br>Dieser Befehl hat etwa folgende Ausgabe:<br>`engwebs01`<br>`engwebs02`<br>`engwebs03` |
| **rsrc show <*Ressourcenname*>** | |
| | Zeigt die Webressourceninformationen für die angegebene Ressource an. Die Ressource muss vorhanden sein; ansonsten wird eine Fehlernachricht angezeigt. Beispiel:<br>`pdadmin> rsrc show engwebs01`<br><br>Dieser Befehl hat etwa folgende Ausgabe:<br>`Web-Ressourcenname: engwebs01`<br>`Beschreibung: Technischer Webserver - Raum 4807` |

# Ressourcengruppen verwalten

Mit den folgenden Befehlen **pdadmin rsrcgroup** können Sie verschiedene ressourcengruppenbezogene Attribute verwalten.

Eine **Ressourcengruppe** bezieht sich auf eine Gruppe von Webservern, bei denen alle Server über dieselben Benutzer-ID- (userids) und Kennwortgruppen verfügen. Sie können eine einzelne Ressourcenberechtigung für alle Ressourcen in der Ressourcengruppe erstellen. Policy Director verwendet eine einzelne Ressourcenberechtigung für eine Ressourcengruppe anstelle einer Ressourcenberechtigung für jede einzelne Ressource in der Ressourcengruppe.

| Befehl | Beschreibung |
| --- | --- |
| **rsrcgroup create <*Ressourcengruppenname*> [–desc <*Beschreibung*>]** | |
| | Erstellt und benennt eine Webressourcengruppe. Das Argument **Ressourcengruppenname** ist der Name der Ressourcengruppe. Das optionale Argument **Beschreibung** kann hinzugefügt werden, um das Identifizieren dieser Ressourcengruppe zu erleichtern. Dem optionalen Parameter **–desc** muss ein Bindestrich (–) vorangestellt werden. Beschreibungen, die Leerzeichen enthalten, müssen zwischen doppelten Anführungszeichen (“) stehen. Beispiel (in einer Zeile eingegeben):<br>pdadmin> rsrcgroup create webs4807 –desc "Webserver, Raum 4807" |
| **rsrcgroup delete <*Ressourcengruppenname*>** | |
| | Löscht die angegebene Ressourcengruppe, einschließlich der Beschreibung. Die Ressourcengruppe muss vorhanden sein. Beispiel:<br>pdadmin> rsrcgroup delete webs4807 |
| **rsrcgroup modify <*Ressourcengruppenname*> add rsrcname <*Ressourcenname*>** | |
| | Fügt einer vorhandenen Ressourcengruppe eine Webressource hinzu. Die Ressourcengruppe muss vorhanden sein. Beispiel (in einer Zeile eingegeben):<br>pdadmin> rsrcgroup modify webs4807 add rsrcname engwebs02 |

<table>
<tr><th>Befehl</th><th>Beschreibung</th></tr>
<tr><td colspan="2"><b>rsrcgroup modify <<i>Ressourcengruppenname</i>> remove rsrcname <<i>Ressourcenname</i>></b></td></tr>
<tr><td></td><td>Löscht eine Webressource aus einer vorhandenen Ressourcengruppe. Beispiel (in einer Zeile eingegeben):<br><code>pdadmin> rsrcgroup modify webs4807 remove</code><br><code>rsrcname engwebs02</code></td></tr>
<tr><td colspan="2">rsrcgroup list</td></tr>
<tr><td></td><td>Zeigt die Namen aller Webressourcengruppen, die im LDAP-Verzeichnis definiert sind, an. Informationen hinter “list” werden ignoriert. Beispiel:<br><code>pdadmin> rsrcgroup list</code><br><br>Dieser Befehl hat etwa folgende Ausgabe:<br><code>webs4807</code><br><code>websbld3</code></td></tr>
<tr><td colspan="2"><b>rsrcgroup show <<i>Ressourcengruppenname</i>></b></td></tr>
<tr><td></td><td>Zeigt die Webressourcengruppeninformationen für die angegebene Ressourcengruppe an. Die Ressourcengruppe muss vorhanden sein; ansonsten wird eine Fehlernachricht angezeigt. Beispiel:<br><code>pdadmin> rsrcgroup show webs4807</code><br><br>Dieser Befehl hat etwa folgende Ausgabe:<br><code>Name der Ressourcengruppe: webs4807</code><br><code>Beschreibung: Webserver, Raum 4807</code><br><code>Ressourcen-Member:</code><br><code>engwebs01</code><br><code>engwebs02</code><br><code>engwebs03</code></td></tr>
</table>

## Ressourcenberechtigungen verwalten

Mit den folgenden Befehlen **pdadmin rsrccred** können Sie verschiedene ressourcenberechtigungsbezogene Attribute verwalten.

Eine **Ressourcenberechtigung** liefert eine Benutzer-ID und ein Kennwort für eine GSO-Benutzerspezifische Ressource, z. B. ein Webserver oder eine Webservergruppe.

Sie können nur die Ressourcenarten “web” und “group” bei Verwendung des Befehls **pdadmin rsrccred** angeben.

**Anmerkung:** Die Ressource oder Ressourcengruppe muss vorhanden sein, damit Sie die Ressourcenberechtigungsbefehle für sie anwenden können.

<table>
<tr><th>Befehl</th><th>Beschreibung</th></tr>
<tr><td colspan="2"><b>rsrccred create <<i>Ressourcenname</i>> rsrcuser <<i>Ressourcenbenutzer-ID</i>> rsrcpwd <<i>Ressourcenkennwort</i>> rsrctype {web|group} user <<i>Benutzername</i>></b></td></tr>
<tr><td></td><td>Erstellt und benennt eine Ressourcenberechtigung. Sowohl Benutzer als auch Ressource (oder Ressourcengruppe) muss bereits vorhanden sein, damit die Ressourcenberechtigung erstellt werden kann. Ist Benutzer, Ressource oder Ressourcengruppe nicht vorhanden oder nicht angegeben, wird eine Fehlernachricht angezeigt. Zu den Ressourcenarten gehören bei den Befehlen für die Ressourcenberechtigungsverwaltung nur die Ressourcen “web” und “group”. Das Argument Ressourcenname ist der Name, den die Ressource bei ihrer Erstellung erhielt. Beispiel:<br><code>engwebs01)</code><br><br>Das Argument Ressourcenbenutzer-ID ist die eindeutige Benutzer-ID für den Benutzer auf dem Webserver. Beispiel:<br><code>4807ws01</code><br><br>Das Argument Ressourcenkennwort ist das Kennwort für einen Benutzer auf dem Webserver. Beispiel:<br><code>rsrpwd</code><br><br>Das Argument Benutzername ist der Name des Benutzers, für den die Ressourcenberechtigungsinformationen gelten. Beispiel:<br><code>dlucas</code><br><br>Beispiel (in einer Zeile eingegeben):<br><code>pdadmin> rsrccred create engwebs01 rsrcuser 4807ws01 rsrcpwd rsrpwd rsrctype web user dlucas</code></td></tr>
</table>

| Befehl | Beschreibung |
| --- | --- |
| **rsrccred modify <*Ressourcenname*> rsrctype {web\|group} set [–rsrcuser <*Ressourcenbenutzer-ID*>] [–rsrcpwd <*Ressourcen-kennwort*>] user <*Benutzername*>** | |
| | Ändert die Benutzer-ID und das Kennwort der Ressourcenberechtigung für die angegebene Ressource. Soll die Ressourcenbenutzer-ID der Benutzer- oder Kennwortinformationen geändert oder zurückgesetzt werden, muss diesen optionalen Befehlen ein Bindestrich (–) vorangestellt werden. Damit die Ressourcenberechtigungsinformationen geändert werden können, müssen die Ressource oder Ressourcengruppe und der Benutzer bereits vorhanden sein. Die angegebene Ressourcenart muss der Ressourcenart entsprechen, die bei der Ersterstellung zugeordnet wurde (z. B. “web” oder “group”). Beispiel (in einer Zeile eingegeben):<br>`pdadmin> rsrccred modify engwebs01 rsrctype group set –rsrcuser 4807ws01 –rsrcpwd newrsrpw user dlucas` |
| **rsrccred delete <*Ressourcenname*> rsrctype {web\|group} user <*Benutzername*>** | |
| | Löscht nur die Ressourcenberechtigungsinformationen für einen vorhandenen Benutzer. Die Ressourcenart muss der Ressourcenart entsprechen, die bei der Erstellung der Ressource zugeordnet wurde (z. B. “web” oder “group”). Beispiel (in einer Zeile eingegeben):<br>`pdadmin> rsrccred delete engwebs01 rsrctype group user dlucas` |
| **rsrccred list user <*Benutzername*>** | |
| | Zeigt die Namen aller definierten Ressourcen und ihre Art für den angegebenen Benutzer an. Beispiel:<br>`pdadmin> rsrccred list user dlucas`<br><br>Dieser Befehl hat etwa folgende Ausgabe:<br>`Ressourcenname: engwebs01`<br>`Ressourcenart: group`<br>`Ressourcenname: engwebs02`<br>`Ressourcenart: web` |

| Befehl | Beschreibung |
|---|---|
| **rsrccred show <*Ressourcenname*> rsrctype {web\|group} user <*Benutzername*>** | |
| | Zeigt die Ressourcenberechtigungsinformationen für einen angegebenen Benutzer an. Ressourcenberechtigung und Benutzer müssen vorhanden sein; ansonsten wird eine Fehlernachricht angezeigt. Beispiel (in einer Zeile eingegeben):<br>`pdadmin> rsrccred show webs4807 rsrctype group user dlucas`<br><br>Dieser Befehl hat etwa folgende Ausgabe:<br>`Ressourcenname: engwebs01`<br>`Ressourcenart: group`<br>`Ressourcenbenutzer-ID: dlucas` |

# Policy-Verwaltungsbefehle

Die Befehle **pdadmin policy** sind eine Gruppe von Verwaltungsbefehlen, die bestimmte Regeln und Bedingungen für LDAP-Benutzer- und -gruppenkonten festlegen.

Sie können folgende Policy-Attribute verwalten:

- Anmeldungs-Policies verwalten
- Kennwort-Policies verwalten

Eine Policy definiert die Bedingungen, die LDAP-Benutzerkonten und -Kennwörtern auferlegt werden, um die Gesamtsicherheit des Systems zu verbessern. Diese Bedingungen können allgemein (global für alle Benutzer im System) oder spezifisch (nur für einen bestimmten Benutzer) auferlegt werden.

Wenn für einen Benutzer eine spezifische Policy gültig ist, hat diese spezifische Policy Vorrang vor allen allgemeinen Policies, die außerdem definiert sein können. Die Vorrangstellung ist unabhängig davon, ob die spezifische Policy restriktiver ist als die allgemeine Policy oder nicht.

## Anmeldungs-Policies verwalten

Mit den folgenden Befehlen **pdadmin policy** können Sie anmeldungsbezogene Policies verwalten.

Mit den anmeldungsbezogenen **Policy**-Verwaltungsbefehlen erstellen Sie neue Anmeldungs-Policies oder kopieren vorhandene Anmeldungs-Policies. Außerdem können Sie Informationen zur Anmeldungs-Policy eines Benutzerkontos anzeigen.

Für anmeldungsbezogene Policies definiert Policy Director die relative Zeit wie folgt:

**TTT-hh:mm:ss**

Die absolute Zeit wird wie folgt definiert:

**JJJJ-MM-TT-hh:mm:ss**

Dies gilt für Policy-Verwaltungsbefehle für die Registrierungs-datenbank.

<table>
<tr><th>Befehl</th><th>Beschreibung</th></tr>
<tr><td colspan="2"><b>policy set account-expiry-date [unlimited <<i>absolute-Zeit</i>>] [–user <<i>Benutzername</i>>]</b></td></tr>
<tr><td colspan="2"><b>policy get account-expiry-date [–user <<i>Benutzername</i>>]</b></td></tr>
<tr><td></td><td>Verwaltet die Policy, die das absolute Datum und die absolute Zeit, nach dem/der ein Benutzerkonto verfallen soll, steuert. Kann auch verwendet werden, um anzugeben, wann alle Benutzerkonten gleichzeitig verfallen sollen. Beispiel 1 (in einer Zeile eingegeben):<br><code>pdadmin> policy set account-expiry-date 1999-12-30-23:30:00 –user dlucas</code><br><br>Beispiel 2:<br><code>pdadmin> policy get account-expiry-date –user dlucas</code></td></tr>
<tr><td colspan="2"><b>policy set disable-time-interval {<<i>Zahl</i>>|unset|disable} [-user <<i>Benutzername</i>>]</b></td></tr>
<tr><td colspan="2"><b>policy get disable-time-interval [-user <<i>Benutzername</i>>]</b></td></tr>
<tr><td></td><td>Verwaltet die Straf-Policy, die den Zeitraum steuert, über den ein Konto inaktiviert werden soll, wenn die maximale Anzahl fehlgeschlagener Anmeldeversuche erreicht wird. Als Administrator können Sie diese Straf-Policy für einen bestimmten Benutzer oder global für alle Benutzer in der LDAP-Registrierungsdatenbank anwenden. Die Standardeinstellung ist 180.</td></tr>
<tr><td colspan="2"><b>policy set max-login-failures {<<i>Zahl</i>>|unset} [-user <<i>Benutzername</i>>]</b></td></tr>
<tr><td colspan="2"><b>policy get max-login-failures [-user <<i>Benutzername</i>>]</b></td></tr>
<tr><td></td><td>Verwaltet die Policy, die die maximal zulässige Anzahl fehlgeschlagener Anmeldeversuche vor einer Strafe steuert. Dieser Befehl ist abhängig von einer im Befehl policy set disable-time-interval festgelegten Strafe. Als Administrator können Sie diese Policy für einen bestimmten Benutzer oder global für alle Benutzer in der LDAP-Registrierungsdatenbank anwenden. Die Standardeinstellung ist 10.</td></tr>
</table>

<table>
<tr><th>Befehl</th><th>Beschreibung</th></tr>
<tr><td colspan="2"><b>policy set tod-access {<<i>Uhrzeit</i>>|unset} [–user <<i>Benutzername</i>>]</b></td></tr>
<tr><td colspan="2"><b>policy get tod-access [–user <<i>Benutzername</i>>]</b></td></tr>
<tr><td></td><td>Gibt die Uhrzeit an, zu der sich ein (oder alle) Benutzer anmelden kann. Die Uhrzeit hat folgendes Format:<br><{anyday|weekday|<<i>Tagesliste</i>>}>:<br><{anytime|<<i>Zeitspezifikation</i>>-<<i>Zeitspezifikation</i>>}><br>[:{utc|local}]<br><br>Gültige Werte für die Variable ’Tagesliste’ sind Mon, Die, Mit, Don, Fre, Sam, Son. Die Bereichsvariablen ’Zeitspezifikation’ müssen wie folgt ausgedrückt werden: hhmm. Zum Beispiel: 0700-1945. Die optionale Zeitzone ist standardmäßig ’lokal’. (Anmerkung: utc=GMT)</td></tr>
</table>

## Kennwort-Policies verwalten

Mit den folgenden Befehlen **pdadmin policy** können Sie verschiedene kennwortbezogene Policy-Attribute verwalten.

Für kennwortbezogene Policies definiert Policy Director die relative Zeit wie folgt:

**TTT-hh:mm:ss**

Dies gilt für **Policy-**Verwaltungsbefehle.

| Befehl | Beschreibung |
| --- | --- |
| **policy set max-password-age {unset\|<*relative-Zeit*>} [–user <*Benutzername*>]** | |
| **policy get max-password-age [–user <*Benutzername*>]** | |
| | Verwaltet die Policy, die die maximale Zeit bis zum Verfall und bis zu einer erforderlichen Änderung des Kennworts steuert. Die angegebene Zeit kann unbegrenzt oder eine in Tagen, Stunden und Minuten ausgedrückte “relative” Zeit sein. Als Administrator können Sie einen bestimmten Benutzernamen angeben oder die Policy global für alle Benutzer in der Registrierungsdatenbank anwenden. Das Argument **relative-Zeit** ist die maximale Zeit (in Tagen, Stunden und Minuten) mit folgendem Format: TTT-hh:mm:ss.<br>Beispiel 1 (in einer Zeile eingegeben):<br>`pdadmin> policy set max-password-age 031-08:30:00 –user dlucas`<br>Beispiel 2:<br>`pdadmin> policy get max-password-age –user dlucas` |

<table>
<tr><th>Befehl</th><th>Beschreibung</th></tr>
<tr><td colspan="2"><b>policy set max-password-repeated-chars {<<i>Zahl</i>>|unset} [-user <<i>Benutzername</i>>]</b></td></tr>
<tr><td colspan="2"><b>policy get max-password-repeated-chars [-user <<i>Benutzername</i>>]</b></td></tr>
<tr><td></td><td>Verwaltet die Policy, die die maximal zulässige Anzahl Zeichenwiederholungen in einem Kennwort steuert. Als Administrator können Sie diese Policy für einen bestimmten Benutzer oder global für alle Benutzer in der Standardregistrierungsdatenbank anwenden. Die Standardeinstellung ist 2.</td></tr>
<tr><td colspan="2"><b>policy set min-password-alphas {<<i>Zahl</i>>|unset} [-user <<i>Benutzername</i>>]</b></td></tr>
<tr><td colspan="2"><b>policy get min-password-alphas [-user <<i>Benutzername</i>>]</b></td></tr>
<tr><td></td><td>Verwaltet die Policy, die die minimal zulässige Anzahl alphabetischer Zeichen in einem Kennwort steuert. Als Administrator können Sie diese Policy für einen bestimmten Benutzer oder global für alle Benutzer in der Standardregistrierungsdatenbank anwenden. Die Standardeinstellung ist 4.</td></tr>
<tr><td colspan="2"><b>policy set min-password-length {<<i>Zahl</i>>|unset} [-user <<i>Benutzername</i>>]</b></td></tr>
<tr><td colspan="2"><b>policy get min-password-length [-user <<i>Benutzername</i>>]</b></td></tr>
<tr><td></td><td>Verwaltet die Policy, die die Mindestlänge eines Kennworts steuert. Als Administrator können Sie diese Policy für einen bestimmten Benutzer oder global für alle Benutzer in der Standardregistrierungsdatenbank anwenden. Die Standardeinstellung ist 8.</td></tr>
<tr><td colspan="2"><b>policy set min-password-non-alphas {<<i>Zahl</i>>|unset} [-user <<i>Benutzername</i>>]</b></td></tr>
<tr><td colspan="2"><b>policy get min-password-non-alphas [-user <<i>Benutzername</i>>]</b></td></tr>
<tr><td></td><td>Verwaltet die Policy, die die minimal zulässige Anzahl nicht alphabetischer (numerischer) Zeichen in einem Kennwort steuert. Als Administrator können Sie diese Policy für einen bestimmten Benutzer oder global für alle Benutzer in der Standardregistrierungsdatenbank anwenden. Die Standardeinstellung ist 1.</td></tr>
</table>

| Befehl | Beschreibung |
|---|---|
| **policy set password-spaces {yes\|no\|unset} [-user <*Benutzername*>]** | |
| **policy get password-spaces [-user <*Benutzername*>]** | |
| | Verwaltet die Policy, die steuert, ob ein Kennwort Leerzeichen enthalten darf. Als Administrator können Sie diese Policy für einen bestimmten Benutzer oder global für alle Benutzer in der Standardregistrierungsdatenbank anwenden. Die Standardeinstellung ist ’nicht definiert’. |

# B

# Referenz für ivmgrd.conf

**Konfigurationsdatei ivmgrd.conf** für den Policy Director Management Server (**pdmgrd**).

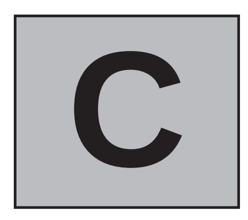
Zeilengruppen:

- [ivmgrd]
- [ldap]
- [ssl]
- [authentication-mechanisms]
- [object-spaces]
- [aznapi-configuration]
- [aznapi-entitlement-services]
- [aznapi-pac-services]
- [aznapi-cred-modification-services]
- [aznapi-external-authzn-services]
- [delegated-admin]

| Parameter | Beschreibung |
| --- | --- |
| Zeilengruppe **[ivmrgd]** | |
| **unix-user** | UNIX-Benutzerkonto für diesen Server. |
| **unix-group** | UNIX-Gruppenkonto für diesen Server. |
| **database-path** | Position der Hauptberechtigungsdatenbank. |
| **tcp-req-port** | TCP-Empfangs-Port für eingehende Anforderungen. |
| **max-notifier-threads** | Maximale Anzahl der Ereignisbenachrichtigungs-Threads. |
| **auto-database-update-notify** | Automatische oder manuelle Aktualisierungsbenachrichtigung für Berechtigungsdatenbankreplikationen aktivieren. |
| **notifier-wait-time** | Inaktivitätszeit (in Sekunden) der Berechtigungs-Policy-Datenbank, bevor die Datenbankreplikationen eine Benachrichtigung erhalten. |
| **pid-file** | Position der PID-Datei. |
| **log-file** | Position der Protokolldatei. |
| **ca-cert-download-enabled** | Clients das Herunterladen des Root-CA-Zertifikats gestatten. |
| Zeilengruppe **[ldap]** | |
| **ldap-server-config** | Position der Konfigurationsdatei `ldap.conf`. |
| **prefer-readwrite-server** | Die Auswahlmöglichkeit des Clients, den LDAP-Server mit Lese-/Schreibzugriff vor der Abfrage von Replikationsservern mit Lesezugriff, die in der Domäne konfiguriert sind, abzufragen aktivieren bzw. inaktivieren. |
| **bind-dn** | Der beim Binden an den LDAP-Server verwendete LDAP-Benutzer-DN. |
| **bind-pwd** | Das LDAP-Benutzerkennwort. |
| **ssl-enabled** | SSL-Übertragung mit dem LDAP-Server aktivieren bzw. inaktivieren. |
| **ssl-keyfile** | Position der SSL-Schlüsseldatei, mit der Zertifikate für die LDAP-Übertragung bearbeitet werden. |

| Parameter | Beschreibung |
|---|---|
| **ssl-keyfile-dn** | Zertifikatkennsatz in der SSL-Schlüsseldatei. |
| **ssl-keyfile-pwd** | Kennwort der SSL-Schlüsseldatei. |
| **auth-using-compare** | Auswählen, ob ldap_compare() anstelle des Aufrufs ldap_bind() zum Authentifizieren von LDAP-Benutzern verwendet wird. |
| Zeilengruppe **[ssl]** | |
| **ssl-keyfile** | Position der SSL-Schlüsseldatei. |
| **ssl-keyfile-pwd** | Kennwort zum Schutz privater Schlüssel in der Schlüsseldatei. |
| **ssl-keyfile-stash** | Position der SSL-Kennwort-Stash-Datei. |
| **ssl-keyfile-label** | Zu verwendender Kennsatz des Schlüssels; nicht der Standardwert. |
| **ssl-v3-timeout** | Sitzungszeitlimit für SSL v3-Verbindungen. |
| **ssl-listening-port** | TCP-Port für den Empfang eingehender MTS-Anforderungen. |
| **ssl-io-inactivity-timeout** | Bei einer SSL-Verbindung der Zeitraum (in Sekunden) bis zur Zeitlimitüberschreitung, wenn auf eine Antwort gewartet wird. |
| **ssl-maximum-worker-threads** | Maximale Anzahl Threads, die der Server zur Bearbeitung eingehender Anforderungen erstellt. |
| **ssl-pwd-life** | Lebensdauer des SSL-Kennworts in Tagen. |
| **ssl-cert-life** | Lebensdauer des SSL-Zertifikats in Tagen. |
| **ssl-auto-refresh** | Automatische Aktualisierung des SSL-Zertifikats und des Kennworts der Schlüsseldatenbankdatei aktivieren bzw. inaktivieren. Bei einer Aktivierung werden das Zertifikat und das Kennwort kurz vor dem Ablauf neu generiert. |
| Zeilengruppe **[authentication-mechanisms]** | |
| **passwd-uraf** | Bibliothek für die Authentifizierung. |
| **cert-uraf** | Bibliothek für die Authentifizierung. |
| **passwd-ldap** | Bibliothek für die Authentifizierung. |
| **cert-ldap** | Bibliothek für die Authentifizierung. |

| Parameter | Beschreibung |
| --- | --- |
| Zeilengruppe **[aznapi-configuration]** | |
| **logsize** | Überlaufschwellenwert der Protokolldatei für Prüfprotokolle. |
| **logflush** | Häufigkeit des zwangsweisen Schreibens in Protokolldateipuffer für Prüfprotokolle. |
| **logaudit** | Prüfung aktivieren bzw. inaktivieren. |
| **auditlog** | Position der Prüfprotokolldatei. |
| **auditcfg = azn** | Berechtigungsereignisse erfassen. |
| **auditcfg = authn** | Authentifizierungsereignisse erfassen. |
| **auditcfg = mgmt** | Authentifizierungsereignisse erfassen. |
| Zeilengruppe **[aznapi-entitlement-services]** | |
| | |
| Zeilengruppe **[aznapi-pac-services]** | |
| | |
| Zeilengruppe **[aznapi-cred-modification-services]** | |
| | |
| Zeilengruppe **[aznapi-external-authzn-services]** | |
| | |
| Zeilengruppe **[delegated-admin]** | |
| **authorize-group-list** | Berechtigungsprüfungen für die Befehle **group list** und **group list-dn** aktivieren bzw. inaktivieren. |



# Referenz für ivacld.conf

**Konfigurationsdatei ivacld.conf** für den Policy Director Authorization Server (**pdacld**).

Zeilengruppen:

- [ivacld]
- [ldap]
- [ssl]
- [manager]
- [authentication-mechanisms]
- [aznapi-configuration]
- [aznapi-entitlement-services]
- [aznapi-pac-services]
- [aznapi-cred-modification-services]
- [aznapi-admin-services]

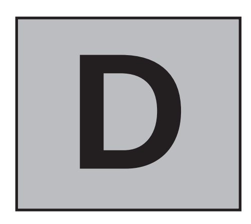
| Parameter | Beschreibung |
|---|---|
| Zeilengruppe **[ivacld]** | |
| **tcp-req-port** | TCP-Empfangs-Port für eingehende Anforderungen. |
| **pid-file** | Position der PID-Datei. |
| **log-file** | Position der Protokolldatei. |

| Parameter | Beschreibung |
|---|---|
| **unix-user** | UNIX-Benutzerkonto für diesen Server. |
| **unix-group** | UNIX-Gruppenkonto für diesen Server. |
| **permit-unauth-remote-caller** | Gibt an, ob Berechtigungs-API-Clients durch den Berechtigungsserver berechtigt werden sollen, bevor ihre Anforderungen verarbeitet werden. |
| Zeilengruppe **[ldap]** | |
| **enabled** | LDAP-Benutzerregistrierungsdatenbankunterstützung aktivieren bzw. inaktivieren. |
| **host** | Host-Name des LDAP-Servers. |
| **port** | Der beim Binden an den LDAP-Server verwendete IP-Port. |
| **bind-dn** | Der beim Binden an den LDAP-Server verwendete LDAP-Benutzer-DN. |
| **bind-pwd** | Das LDAP-Benutzerkennwort. |
| **cache-enabled** | Zwischenspeichern von LDAP-Client-Daten zur Verbesserung des Durchsatzes für ähnliche LDAP-Abfragen aktivieren bzw. inaktivieren. |
| **prefer-readwrite-server** | Die Auswahlmöglichkeit des Clients, den LDAP-Server mit Lese-/Schreibzugriff vor der Abfrage von Replikationsservern mit Lesezugriff, die in der Domäne konfiguriert sind, abzufragen aktivieren bzw. inaktivieren. |
| **ssl-enabled** | SSL-Übertragung mit dem LDAP-Server aktivieren bzw. inaktivieren. |
| **ssl-keyfile** | Position der SSL-Schlüsseldatei, mit der Zertifikate für die LDAP-Übertragung bearbeitet werden. |
| **ssl-keyfile-dn** | Zertifikatkennsatz in der SSL-Schlüsseldatei. |

| Parameter | Beschreibung |
|---|---|
| **ssl-keyfile-pwd** | Kennwort der SSL-Schlüsseldatei. |
| **max-search-size** | Maximale Größe des Suchpuffers, die vom LDAP-Server in Einträgen zurückgegeben wird. |
| **ssl-port** | Empfangsbereiter SSL-Port für LDAP-Übertragung. |
| **auth-using-compare** | Auswählen, ob ldap_compare() anstelle des Aufrufs ldap_bind() zum Authentifizieren von LDAP-Benutzern verwendet wird. |
| **ldap-replica** | Die LDAP-Benutzerregistrierungs-datenbankreplikationen in der Domäne definieren. |
| Zeilengruppe **[ssl]** | |
| **ssl-keyfile** | Position der SSL-Schlüsseldatei. |
| **ssl-keyfile-pwd** | Kennwort zum Schutz privater Schlüssel in der Schlüsseldatei. |
| **ssl-keyfile-stash** | Position der SSL-Kennwort-Stash-Datei. |
| **ssl-keyfile-label** | Zu verwendender Kennsatz des Schlüssels; nicht der Standardwert. |
| **ssl-v3-timeout** | Sitzungszeitlimit für SSL v3-Verbindungen. |
| **ssl-listening-port** | TCP-Port für den Empfang eingehender MTS-Anforderungen. |
| **ssl-io-inactivity-timeout** | Bei einer SSL-Verbindung der Zeitraum (in Sekunden) bis zur Zeitlimitüberschreitung, wenn auf eine Antwort gewartet wird. |
| **ssl-maximum-worker-threads** | Maximale Anzahl Threads, die der Server zur Bearbeitung eingehender Anforderungen erstellt. |
| **ssl-pwd-life** | Lebensdauer des SSL-Kennworts in Tagen. |

| Parameter | Beschreibung |
|---|---|
| **ssl-cert-life** | Lebensdauer des SSL-Zertifikats in Tagen. |
| **ssl-auto-refresh** | Automatische Aktualisierung des SSL-Zertifikats und des Kennworts der Schlüsseldatenbankdatei aktivieren bzw. inaktivieren. Bei einer Aktivierung werden das Zertifikat und das Kennwort kurz vor dem Ablauf neu generiert. |
| **ssl-authn-type** | Authentifizierungsart. |
| Zeilengruppe **[manager]** | |
| **manager-host** | Host-Name des MTS-Servers. |
| **master-port** | TCP-Port, an dem der Server empfangsbereit für Anforderungen ist. |
| **master-dn** | Der vom MTS-Server dargestellte und erwartete registrierte Name des Zertifikats. |
| Zeilengruppe **[authentication-mechanisms]** | |
| **passwd-uraf** | Bibliothek für die Authentifizierung. |
| **cert-uraf** | Bibliothek für die Authentifizierung. |
| **passwd-ldap** | Bibliothek für die Authentifizierung. |
| **cert-ldap** | Bibliothek für die Authentifizierung. |
| Zeilengruppe **[aznapi-configuration]** | |
| **logsize** | Überlaufschwellenwert der Protokolldatei für Prüfprotokolle. |
| **logflush** | Häufigkeit des zwangsweisen Schreibens in Protokolldateipuffer für Prüfprotokolle. |
| **logaudit** | Prüfung aktivieren bzw. inaktivieren. |
| **auditlog** | Position der Prüfprotokolldatei des lokalen Clients. |
| **auditcfg = azn** | Berechtigungsereignisse erfassen. |
| **auditcfg = authn** | Authentifizierungsereignisse erfassen. |

| Parameter | Beschreibung |
|---|---|
| **db-file** | Position der Datenbank-Cache-Datei pdacld. |
| **cache-refresh-interval** | Das Aktualisierungsprüfintervall für den Master Authorization Server. |
| **permission-info-returned** | |
| **max-handle-groups** | Maximale Anzahl zuzuordnender Kennungsgruppen. |
| **listen-flags** | Den Empfang von Policy-Cache-Aktualisierungsbenachrichtigungen aktivieren bzw. inaktivieren. |
| Zeilengruppe **[aznapi-entitlement-services]** | |
| | Definiert Berechtigungs-API-Services. |
| Zeilengruppe **[aznapi-pac-services]** | |
| **AZN_V37CRED_SVC** | Ein Service für die Konvertierung zwischen Policy Director 3.7-Berechtigungen und Policy Director 3.8-Berechtigungen. Gestattet die Unterstützung ferner Berechtigungsanforderungen von Policy Director 3.7-Berechtigungs-API-Anwendungen. |
| Zeilengruppe **[aznapi-cred-modification-services]** | |
| **AZN_MOD_SVC_RAD_2AB** | Ein Berechtigungsänderungsservice, mit dem Gruppen einer vorhandenen Berechtigung dynamisch hinzugefügt werden können. Mit dieser Aktion kann der Eigner der Berechtigung zusätzliche Berechtigungsmöglichkeiten erhalten. |
| Zeilengruppe **[aznapi-admin-services]** | |
| **AZN_ADMIN_SVC_TRACE** | Trace-Verwaltung für eine Berechtigungs-API-Anwendung aktivieren bzw. inaktivieren (mit Hilfe von pdadmin). |



# Referenz für ldap.conf

## Konfigurationsdatei ldap.conf

Zeilengruppen:

- [ldap]

| Parameter | Beschreibung |
|---|---|
| Zeilengruppe **[ldap]** | |
| **enabled** | Policy Director verwendet eine LDAP-Benutzer-registrierungsdatenbank. Gültige Werte sind “yes” und “no”. |
| **host** | Der Netzname der Maschine, auf der sich der LDAP-Master-Server befindet. |
| **port** | Der TCP-Empfangs-Port des LDAP-Master-Servers. |
| **ssl-port** | Der SSL-Empfangs-Port des LDAP-Master-Servers. |
| **max-search-size** | Das Policy Director-Limit für eine LDAP-Client-Suche nach Datenbankeinträgen - z. B. eine Anforderung an die Management Console, Benutzer aus der LDAP-Datenbank aufzulisten. |
| **replica** | LDAP-Replikationsservereintrag. |



# Referenz für pd.conf

**Konfigurationsdatei pd.conf**

Zeilengruppen:

- [pdrte]
- [ssl]
- [manager]
- [ldap-ext-cred-tags]

| Parameter | Beschreibung |
|---|---|
| Zeilengruppe **[pdrte]** | |
| **configured** | Gibt an, ob das Paket PDRTE konfiguriert wurde. |
| **user-reg-type** | Art der Benutzerregistrierungsdatenbank. (Momentan wird nur LDAP unterstützt.) |
| **user-reg-server** | Servername der Benutzerregistrierungsdatenbank. |
| **user-reg-host** | Host-Name der Benutzerregistrierungsdatenbank. |
| **user-reg-hostport** | Server-Port-Nummer der Benutzerregistrierungsdatenbank. |
| **boot-start-ivmgrd** | Management Server (pdmgrd) beim Systemstart starten. |

| Parameter | Beschreibung |
| --- | --- |
| **boot-start-ivacld** | Authorization Server (pdacld) beim Systemstart starten. |
| Zeilengruppe **[ssl]** | |
| **ssl-keyfile** | Position der SSL-Schlüsseldatei im lokalen System. |
| **ssl-keyfile-pwd** | Kennwort der Schlüsseldatei. |
| **ssl-keyfile-stash** | Position der SSL-Kennwort-Stash-Datei. |
| **ssl-keyfile-label** | Zu verwendender Name des Zertifikats; nicht der Standardwert. |
| **ssl-v3-timeout** | Sitzungs-ID-Zeitlimit für SSL v3-Verbindungen. |
| **ssl-pwd-life** | Lebensdauer des SSL-Kennworts in Tagen. |
| **ssl-io-inactivity-timeout** | Bei einer SSL-Verbindung der Zeitraum (in Sekunden) bis zur Zeitlimitüberschreitung, wenn auf eine Antwort gewartet wird. |
| **ssl-auto-refresh** | Automatische Aktualisierung der Schlüsseldatenbankzertifikate und -kennwörter aktivieren bzw. inaktivieren. |
| Zeilengruppe **[manager]** | |
| **master-host** | Host-Name des MTS-Servers. |
| **master-port** | Nummer des TCP-Ports, an dem der Server empfangsbereit für Anforderungen ist. |
| **replica** | Authorization Server-Replikationen. |
| Zeilengruppe **[ldap-ext-cred-tags]** | |
| ***<credential-field-name> = <ldap-inetOrgPerson-field>*** | Mechanismus zum Hinzufügen erweiterter Attribute zur Policy Director-Berechtigung aus vorhandenen Feldern in der LDAP-Objektklasse inetOrgPerson. |

# Index

## Sonderzeichen



## A



## B

## R



## S



## T



## U



## V



## W

## Z




GC12-2958-01

